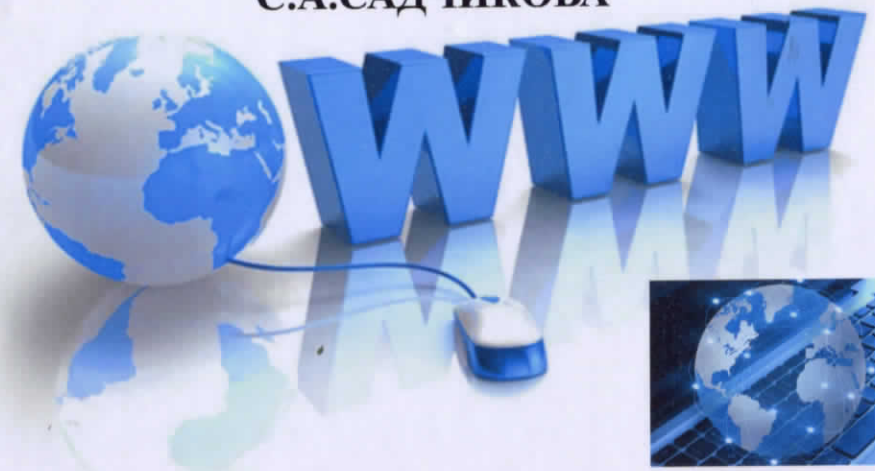
М.Б.АБДУЖАППАРОВА,
С.А.САДЧИКОВА




# ИНТЕРНЕТ
# СЕТИ И УСЛУГИ

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРЕЗМИ

**М.Б.АБДУЖАППАРОВА, С.А.САДЧИКОВА**

# ИНТЕРНЕТ СЕТИ И УСЛУГИ

**(Учебник)**

Ташкент-2019

**УДК: 004**
**ББК: 32.973.202**

**М.Б.Абдужаппарова, С.А.Садчикова. Интернет сети и услуги. (Учебник). – Т.:"Aloqachi", 2019. – 300 с.**

**ISBN 978-9943-6395-1-5**

В данном учебнике рассмотрены принципы построения сети Интернет, составляющие компоненты сети, методы подключения пользователей в сети Интернет, технические характеристики технологий доступа, принципы передачи данных в IP сети, применение модели сети OSI в сети Интернет, сетевые протоколы, создание и принципы предоставления Интернет-услуг.

Учебник предназначен для студентов всех направлений Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми и инженеров учреждений телекоммуникационной отрасли Республики Узбекистан.

**УДК: 004**
**ББК: 32.973.202**

***Рецензенты:*** Шарифов Р.А. к.т.н., доцент, директор ООО "ISKRATEL TASHKENT"

Гультураев Н.Х. к.т.н., доцент каф. «ТИ» Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми.

**ISBN 978-9943-6395-1-5**





## ПРЕДИСЛОВИЕ

На сегодняшний день в Республике Узбекистан актуальной задачей в системе образования считается требование по обеспечению высококвалифицированными кадрами. Эта задача отмечена в принятых законах «Об образовании» и «Национальной программы при подготовке кадров».

Модернизация метода обучения играет важную роль в повышении качества усвоения изучаемого предмета и поднятии уровня качества обучения, согласно требованиям мировых стандартов в целом.

В Узбекистане год за годом развиваются и широко внедряются в повседневную жизнь информационно–коммуникационные технологии, для жителей Республики стали доступны и привычны не только автономное использование компьютеров, но использование ресурсов сети интернет для собственных целей и развития бизнеса.

Данный учебник предоставит возможность для получения знаний о структуре сети Интернет, принципах её работы, используемых протоколах и предоставляемых сервисах. Ускоренные темпы развития средств современных информационно-коммуникационных технологий дают возможность создания и регулирования информационного общества. В информационном обществе в каждой сфере трудовой активности человека большинство людей занимаются созданием информации, её сохранением и переработкой, где важную роль играют интернет сети и интернет технологии.

Сегодня интернет технологии относятся к глобальной развивающейся сфере. Компьютеры глубоко проникли в жизнь человеческого общества. Без них невозможно представить глобальную сеть Интернет, рабочее место интеллектуального работника. Компьютерные технологии играют важную роль в человеческой жизни малых и больших предприятий, компаний, в учебных заведениях, в государственных учреждениях.

На данный момент в мире статус достойного геополитика оценивается уровнем развития современных компьютерных технологий, телекоммуникационных сетей и систем, методами доступа в информационный мир и их возможностями.

Сегодня глобальные перемены произошли в сфере методов передачи информации по телекоммуникационным сетям с одной

точки земного шара на другую. Этот обмен информацией обеспечивается Всемирной сетью.

Данный учебник предназначен не только студентам всех направлений Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми, инженерам учреждений телекоммуникационной отрасли Республики Узбекистан, но и всем интересующимся структурой сети Интернет, принципами её работы и сервисами, предоставляемыми сетью.



## ВВЕДЕНИЕ

Коммуникационные технологии играют важнейщую роль в жизни общества и экономики. В Республике Узбекистан принята комплексная программа по развитию национальной информационно-коммуникационной системы на 2013-2020 г.г.

Данная комплексная программа обеспечивает общество информационно-коммуникационными продуктами и их услугами, которыми могут пользоваться каждая семья и все общество. Модернизация отрасли телекоммуникации привела к экономическому развитию государства, интернет услуги проникают в каждую семью, день за днём повышается скорость доступа к сети интернет.

Большое внимание уделено развитию и внедрению информационно-коммуникационных технологии для населения, живущих в удалённых районах местности.

Internet – это глобальная компьютерная сеть, работающая по единому стандарту во всем мире. Его название расшифрируется по 2 критериям, то есть, “International Network” – международная сеть и “Interconnected networks” – “межсетевые сети”.

Internet – информационная сеть, соединяющая локальную компьютерную сеть, которая предоставляет возможности им обмена информациями.

Пользователи интернет сети могут передать информации между городами и государствами со своих персональных компьютеров.

Например, в Вашингтоне просмотреть каталог библиотеки Конгрессов, в Нью-Йорке ознокомиться с недавными поставленными фото, участвовать в национальных конференциях, пользоваться банковскими услугами, а также играть в шахматы с жителями других государств.

Основные ячейки компьютерных сетей - это персональные компьютеры и соединяющие их локальные сети.

Internet не только устанавливает связь между компьютерами, но и соединяет группы компьютеров. Если местная сеть подключена к интернет, то все рабочие станции данной сети (компьютеры) могут пользоваться услугами интернет сети.

Также, в интернет сети есть самостоятельно подключенные компьютеры, их называют хост компьютеры (host – основная вычислительная машина). У каждых компьютеров, подключённых к

сети есть свой адрес и с помощью их можно общаться с любой точки земли с любым пользователем.

Internet – управляюшая сложнейщая система, включающая техническую, программную и информационную часть.

Техническое обеспечение интернет сети включает в себя разные типы компьютеров и каналов связи (телефон, спутник, опто-волокно и других типов каналов сети), а также комплекс технических средств.

Программное обеспечение интернет сети обеспечивает работоспособность подключённых в сеть разных компьютеров и сетевых средств по единому стандарту.

Информационное обеспечение интернет сети составляет в интернет сетях сушествующие разные электронные документы, график, аудио, видео, веб-сайты и др. видов комплексов информации.

У Интернета есть две основные задачи:

- информационная часть,
- коммуникационное средство.

Задачей интернет сети является чтение Beb-документов, электронная почта, передача и приём файлов, сохранение документов на сети и работа над этими документами.

В Интернет сети можно пользоваться обменом информацией, дистанционным обучением, проведением конференции, создание веб-сайтов, создание электронной почты и в других целях.

В данном учебнике рассмотрены принципы построения сетей интернет, их компоненты, методы подключения пользователей в сети интернет, их технические характеристики, технологии интернет сети, принципы передачи данных в сети интернет, модель сети OSI в сетях интернет, сетевые протоколы и создание Internet услуг.



# 1. КОМПЬЮТЕРНЫЕ СЕТИ И ИНТЕРНЕТ

## 1.1. Введение – что такое Интернет?

Компьютерная сеть – это два и более компьютеров, соединенных линиями передачи информации (см.рис.1.1). Различают локальные и глобальные компьютерные сети.

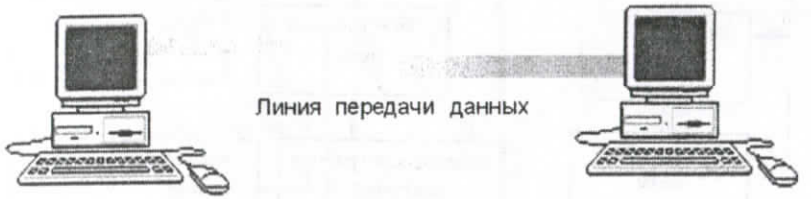



Рис.1.1. Простейшая компьютерная сеть

Скорость передачи информации (пропускная способность канала) - количество информации в битах в секунду (бит/с) и в производных единицах (кбит/с, Мбит/с, Гбит/с). Принято следующее соотношение: 1кбит/с = 1024бит/с; 1Мбит/с = 1024кбит/с; 1Гбит/с = 1024Мбит/с.

Понятие «компьютерные коммуникации» включает в себя несколько компонентов, таких как типы компьютерных сетей, аппаратные средства сети, сетевое программное обеспечение, услуги сети (см.рис.1.2).

По типам компьютерных сетей различают локальные и глобальные сети. Локальная компьютерная сеть объединяет компьютеры, установленные в одном помещении. Локальная сеть позволяет пользователям получить совместный доступ к ресурсам компьютеров, а также к периферийным устройствам (принтерам, сканерам, дискам, модемам и др.), подключенным к сети. Глобальная компьютерная сеть – это система связанных между собой компьютеров, расположенных на большом удалении друг от друга. Глобальная сеть позволяет организовать информационное общение между абонентами на больших расстояниях в масштабах всей планеты. Её основу составляют региональные и корпоративные сети. Региональные сети объединяют компьютеры в пределах региона: города, области, края, страны. Корпоративные сети обеспечивают деятельность предприятий (филиалы, представительства).

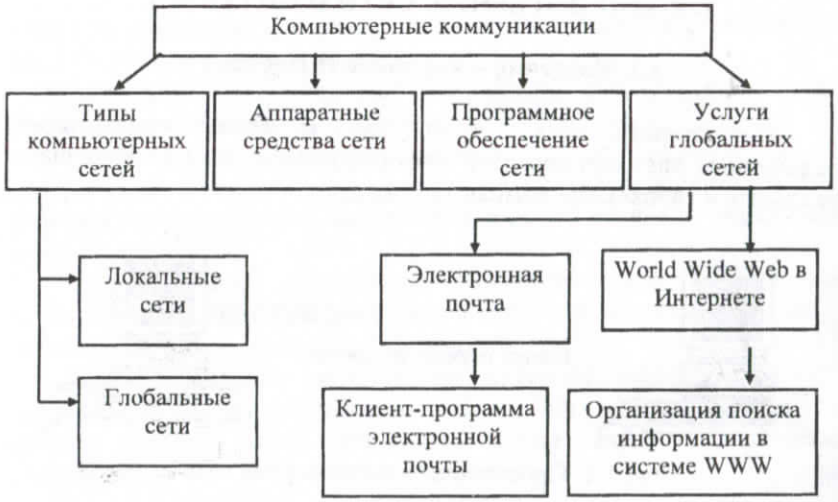



Рис.1.2. Составные части понятия «компьютерные коммуникации»

**Интернет** – это глобальная компьютерная (телекоммуникационная) сеть – объединение многих локальных сетей и отдельных компьютеров, находящихся на больших расстояниях друг от друга. Телекоммуникации - процесс обмена информации по глобально сети.

Интернет объединяет многочисленные локальные, региональные и корпоративные сети, а также компьютеры отдельных пользователей, распределённые по всему миру. Основой сети Интернет являются компьютерные узлы и каналы связи. **Узел** - это мощный компьютер, постоянно подключённый к сети.

Физические каналы для передачи данных бывают на основе электрического кабеля, оптоволоконного кабеля, радиосвязи, инфракрасных лучей, линий телефонной сети.

К узлам компьютерной сети подключаются **абоненты** - персональные компьютеры пользователей или локальные сети. Организация, предоставляющая пользователям связь с Интернет через свои компьютеры, называется **провайдером** (provider - поставщик) сетевых услуг.



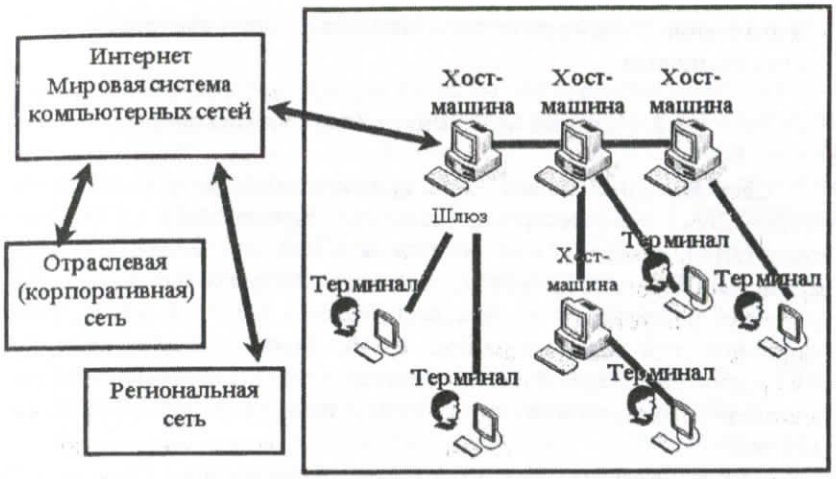



Рис.1.3. Архитектура глобальной сети

Определение «Интернет» было дано в 1995г. федеральным Сетевым Советом США (FNC или Federal Networking Counsil):
«Интернет — это часть глобальной информационной системы, которая:

- логически связана унитарным адресным пространством, основанном на IP протоколе или на его перспективных расширениях;
- может поддерживать коммуникации, используя Transmission Control Protocol/ Internet Protocol (TCP/IP) или его расширения/последователи и/или IP-совместимые протоколы;
- предоставляет, использует или делает доступными (для всех или конфиденциально) сервисы высокого уровня, основанные на коммуникациях и связанной с ними инфраструктуре, здесь определенной».

Тогда же были сформулированы основные правила технологии Интернет:

- Интернет – самая большая глобальная сеть, охватывает весь мир.
- Интернет – объединение сетей разных организаций и операторов связи.
- В Интернете нет единого центра.

– Управление Интернетом ведется неправительственными организациями.

### 1.2. История возникновения сети Интернет

Сеть Интернет начала свое существование с сети ARPANet в 1969г. Эта компьютерная сеть с применением технологии коммутации пакетов была создана в США по заданию военного ведомства США как высоконадежная сеть передачи данных. В 1983г. ARPANet разделилась на две сети, одна - MILNET стала частью оборонной сети передачи данных США, другая - была использована для соединения академических и исследовательских центров, которая постепенно развивалась и в 1990 году трансформировалась в Интернет.

Таким образом, можно сделать вывод, что сеть Интернет возникла из оборонного проекта конца 60-х – начала 70-х г.г. XXв., направленного на создание коммуникационной сети, способной функционировать даже в условиях атомной войны. По мнению разработчиков, наиболее важное качество сети - отсутствие единого центра управления, который мог бы стать объектом нападения. Была создана анархичная сеть, в которой одна вычислительная машина не более важна, чем любая другая, и ни один компьютер не является жизненно важным для функционирования сети в целом. Последующее распространение использования Internet в области исследований, коммерции и досуга было неожиданным следствием этого проекта.

В 1961г. Defence Advanced Research Agensy (DARPA) по заданию министерства обороны США приступило к проекту по созданию экспериментальной сети передачи пакетов. Эта сеть, названная ARPANet, предназначалась первоначально для изучения методов обеспечения надежной связи между компьютерами различных типов. В 1972г. - Первая демонстрация ARPANet, Р.Томпсон изобрёл электронную почту. Тогда же были разработаны и протоколы передачи данных в сети - TCP/IP. TCP/IP - это множество коммуникационных протоколов, которые определяют, как компьютеры различных типов могут общаться между собой.

1973г. Р.Кан и В.Серф излагают идею структуры Internet, и производятся первые подсоединения к сети извне США. Эксперимент с ARPANet был настолько успешен, что многие организации захотели



войти в нее, с целью использования для ежедневной передачи данных.

В 1975г. ARPANet превратилась из экспериментальной сети в рабочую сеть. Ответственность за администрирование сети взяло на себя Defence Communication Agency (DCA), в настоящее время называемое Defence Information Systems Agency (DISA). Но развитие ARPANet на этом не остановилось; Протоколы TCP/IP продолжали развиваться и совершенствоваться. В 1977г. первым 100 исследователям была обеспечена услуга электронной почты.

В 1983г. вышел первый стандарт для протоколов TCP/IP, вошедший в Military Standarts (MIL STD), т.е. в военные стандарты, и все, кто работал в сети, обязаны были перейти к этим новым протоколам. **Этот год считается годом рождения сети Internet**. Для облегчения этого перехода DARPA обратилась с предложением к руководителям фирмы Berkley Software Design - внедрить протоколы TCP/IP в Berkeley (BSD) UNIX. С этого и начался союз UNIX и TCP/IP. Спустя некоторое время TCP/IP был адаптирован в обычный общедоступный стандарт, и термин Internet вошел во всеобщее употребление.

Когда в 1983г. из ARPANET выделилась MILNET, которая стала относиться к Defence Data Network (DDN) министерства обороны США, термин Internet стал использоваться для обозначения единой сети: MILNET плюс ARPANET.

В 1984г. в сеть Интернет включено 1000 машин, 1989г. – 100тыс., в 1992 г. в Internet включено уже 1000 000 машин.

В 1992г. Тим Бернес-Ли изобретает «Всемирную Паутину» WWW. Формируется общество Internet ISOS. Создание World Wide Web явилось важным событием в истории Интернет. Идея, предложена физиком Европейской организации ядерных исследований (ЦЕРН Женева), заключалась в том, чтобы позволить физикам и другим учёным пользоваться распределённой в сети Интернет информацией более простым способом. Существовавшие тогда средства Интернет требовали от пользователей немалых знаний о сети, поэтому был разработан новый метод передачи и отображения информации. После опубликования ЦЕРН спецификаций для WWW пользователи стали писать программное обеспечение для клиентов и серверов WWW, что привело к созданию «Всемирной паутины» в том виде, в котором она известна сегодня.

Третьим важным событием в истории Интернет была разработка

группой программистов из Национального центра компьютерных приложений NCSA первой программы-браузера MOSAIC, которая окончательно сделала Интернет общедоступной сетью. Браузер MOSAIC позволил пользователям получать и отображать документы простым нажатием кнопки «мыши». Отпала необходимость заботиться о переключении программ и преобразовании файлов. Программа-браузер обрабатывала документы, графики, изображения и звуки автоматически, обеспечивая лёгкий доступ к WWW. Безликая, в основном текстовая, с трудно отыскиваемыми ресурсами, сеть превратилась в полноцветный и легкодоступный источник различной информации, от простого текста до видеофильмов.

В 1991г. ARPANET прекратила свое существование, сеть Internet существует, ее размеры намного превышают первоначальные, так как она объединила множество сетей во всем мире. Сеть ARPANET первоначально состояла всего из 4 больших ЭВМ. 1995г. - более 4,5 млн. активных компьютеров. Основной рост пользователей 90-е г.г. XXв., когда развивалась инфраструктура коммуникаций и возросли возможности компьютеров. В 25 годовщину ARPANET/Internet сеть стала использоваться для маркетинга, покупок, банковских операций, радиовещания и «живых» концертов.

1995г. порталы Compuserve, Progidy, America Online начинают обеспечивать широкомасштабный доступ в Internet. В это время появляется и завоёвывает широкую популярность программа-браузер Netscape Navigator.

До середины 1990 годов Интернет был доступен относительно узкому академическому сообществу, а его наполнение не отличалось богатством и разнообразием. В настоящее время на десятках миллионов компьютеров, подключенных к Интернету, хранится громадный объем информации (сотни миллионов файлов, документов и т. д.) и сотни миллионов людей пользуются информационными услугами глобальной сети. Основу, «каркас» Интернета составляют более ста миллионов серверов, постоянно подключенных к сети. К серверам Интернета могут подключаться с помощью локальных сетей или коммутируемых телефонных линий сотни миллионов пользователей сети. В каждой локальной или корпоративной сети обычно имеется, по крайней мере, один компьютер, который имеет постоянное подключение к Интернету с помощью линии связи с высокой пропускной способностью (сервер Интернета).



**Каковы перспективы сети Интернет в Новом тысячелетии?**
Инновации в компьютерных сетях продолжаются быстрыми темпами. Прогресс достигается на всех фронтах, включая развертывание более быстрых маршрутизаторов и более высоких скоростей передачи информации как в сетях доступа, так и в сетевых магистралях. Однако особого внимания заслуживают следующие события:

- С начала тысячелетия мы наблюдаем активное развертывание широкополосного доступа в Интернет в домах – не только кабельных модемов и DSL, но и оптоволокна к дому, как обсуждается в разделах 2.3,2.5. Этот высокоскоростной доступ в Интернет подготавливает почву для реализации и пользования большим числом видео-приложений, таких каксовместный просмотр и распределение созданного пользователями видео (например, YouTube), передача по требованиюфильмов и телевизионных шоу (например, в Netflix, mediabay.uz), многопользовательские видеоконференции (например, Skype).
- Широкое внедрение высокоскоростных (54Мбит/с и выше) сетей Wi-Fi общего пользования и доступ к среднескоростному (до нескольких Мбит/с) интернету через сети сотовой связи 3G и 4G не только позволяет оставаться постоянно подключенными к Сети при движении, но и использовать новые приложения, зависящие от местоположения. По данным мировой статистики в 2011г. количество беспроводных устройств, подключенных к Интернету, превысило количество проводных устройств. Высокоскоростной беспроводный доступ подготовил почву для появления и широкого использования карманных компьютеров (айфоны, андроиды, айпады и так далее), которые пользуются постоянным или мобильным доступом к Сети.
- Интернет-социальные сети, такие как Facebook и Twitter, создали массовые объединения людей на вершине Интернета. Многие интернет-пользователи сегодня «живут» в основном в Facebook. Через свои API социальные сети создают платформы для новых сетевых приложений и распределенных игр. Поставщики онлайн-услуг, такие как Google и Microsoft, развернули свои собственные обширные частные сети, которые не только объединяют их глобально распределенные центры обработки данных, но и используются для создания обходных путей, минуя сеть Интернет, путем прямой передачи данных от источника к отправителю (пиринга) Интернет-провайдерами нижнего уровня. В результате

Google предоставляет результаты поиска и доступ к электронной почте почти мгновенно, как если бы их центры обработки данных работали на собственном компьютере.

- Многие компании интернет-торговли в настоящее время работают над «облачными» приложениями, например, в компании Amazon EC2, поисковой системе Google, или Microsoft Azure. Многие компании и университеты также перенесли свои Интернет-приложения (электронную почту и веб-хостинг) в облачные хранилища информации. Облачные компании не только предоставляют приложениям масштабируемые вычислительные среды и среды хранения, но и предоставляют приложениям неявный доступ к их высокопроизводительным частным сетям.

### 1.2.1. Появление Интернет в Узбекистане

Появление Интернета в Узбекистане произошло практически одновременно с появлением интернета в странах СНГ.

В 1990г. профессиональная научная сеть Института атомной энергии им. И.В.Курчатова и ИПК Минавтопрома, объединившая ученых-физиков и программистов, соединилась с мировой сетью Интернет, положив начало современным российским сетям. В 1990г. был зарегистрирован домен первого уровня .su в базе данных Международного информационного центра InterNIC. В результате этого Советский Союз стал виден всему интернетовскому миру. Российская Федерация подключилась в 1993г. В 1994г. в InterNIC был зарегистрирован уже именно российский домен .ru. С этого момента существование Интернета в Российской Федерации было заверено официально на международном уровне.

Домен «UZ» был зарегистрирован 29 апреля 1995г., но компьютерные сети (в первую очередь сеть «Фидонет») появились в Узбекистане ещё раньше в начале 90г.г. XXв.[1][2]. В 1996г. при Кабинете Министров Республики Узбекистан под эгидой ООН был создан проект по развитию Интернета в Узбекистане, впоследствии известный как UzNet.

[1] Алимова Г.Б. История развития Интернета в Узбекистане: детали, прогнозы // Проблемы филологии, культурологии и искусствоведения в свете современных исследований: сборник материалов 18 международ. науч.-практ. конф. – Махачкала: Издательство «Апробация», 2016. – с.42-44

[2] http://www.xn--h1aekdm.uz/



1997-1999г.г. можно охарактеризовать как эпоху «дикого» развития Интернета. Каждый провайдер имел свой независимый канал для подключения к международным Интернет-провайдерам. Час работы в сети Интернет стоил 600 сум в час (на то время это - около 4 долларов по курсу ЦБ РУз). На абонентском участке для доступа в Интернет использовались технологии работы по выделенным линиям, которые постепенно переходили с аналоговых методов передачи на цифровые. Первые интернет-тарифы имели повременную оплату, т.к. использовали dial-up доступ, в тоже время появляются тарифы доступа в Интернет в зависимости от объёма использованного трафика. Среди пользователей Республики делаются первые попытки использовать Интернет в качестве среды передачи голоса.

В 1999г. было принято решение, что доступ к международным сетям передачи данных, включая Интернет, должен осуществляется только через предприятие по развитию и эксплуатации сети передачи данных «UzPAK» при получении лицензии на право выхода на международные сети от УзАСИ.

В 2001-2002г.г. зафиксирован рост пропускной способности внешнего Интернет-канала с 8,5Мбит/с до 18Мбит/с. Выходит Постановление №352 Кабинета Министров РУз «О децентрализации доступа к международным компьютерным сетям»[3].

2003-2005г.г. характеризуются приходом Российских и крупных международных компаний на рынок сотовой связи Узбекистана, таких как Вымпелком (Билайн), МТС, Telia Sonera. Появляются компании на рынке IP телефонии – Platinum connect, Oxygen, Buzton.

2005г. ознаменован появлением Правительственного портала Республики Узбекистан – www.gov.uz. Постановление Кабинета Министров РУз от 06.10.2005 № 221 возложило функции национального оператора (провайдера) по эксплуатации и развитию сетей передачи данных, включая Интернет, на АК «Узбектелеком»[4]. Была создана Национальная общественная образовательная информационная сеть ZiyoNet, Национальная информационно-поисковая система WWW.UZ.

В 2006-2009г.г. произошло открытие первого Центра регистрации электронной цифровой подписи. Компании начинают

[3] http://lex.uz/pages/GetAct.aspx?lact_id=314306

[4] http://www.medialawca.org/document/-1791

предоставлять услуги беспроводного доступа в Интернет по технологиям GPRS, 3G, Wi-MAX. Количество Интернет-пользователей превышает 2млн., количество пользователей сотовой связи 10млн.

2010-2011г.г. характеризуются всплеском популярности мобильного интернета. Число пользователей Сети составляет 7,378млн., при этом число пользователей мобильного Интернета – 4,119млн. К концу 2010г. количество государственных органов, использующих услуги Интернет, возросло до 7643 единиц. Согласно данным центра Узинфоком число активных доменов, зарегистрированных в зоне «.UZ» по итогам 2010г., превысило число в 11тыс.

В 2012г. по данным Государственного комитета связи, информатизации и телекоммуникационных технологий Республики Узбекистан, количество пользователей сети Интернет (включая число пользователей мобильного интернета) в Узбекистане достигло 9,815млн.[5]. К концу 2014г. этот показатель составляет более 10,2 миллиона человек, или треть всего населения. Пропускная способность интернет-канала внутри республики увеличилась в 4 раза, а скорость доступа – в 1,5 раза.

В первой половине 2016г. число пользователей интернета превысило 12млн. из 31,5 миллионного постоянного населения страны[6].

Не смотря на интенсивное развитие интернета в стране, на основании текущего состояние, мнения провайдеров и мировых тенденций развития всемирной информационной сети можно понять, можно выделить ряд существующих проблем, препятствующих углублению проникновения Интернета в Узбекистане. Например, существует очень большая разница уровня проникновения Интернет в столице и регионах республики.

### 1.3. Принципы построения сети Интернет

Есть несколько способов ответить на вопрос: «что такое Интернет и как построена сеть Интернет»:

[5] http://www.anons.uz/article/it/11281/

[6] Алимова Г.Б. История развития Интернета в Узбекистане: детали, прогнозы // Проблемы филологии, культурологии и искусствоведения в свете современных исследований: сборник материалов 18 международ. науч.-практ. конф. – Махачкала: Издательство «Апробация», 2016. – с.42-44



– с точки зрения основных аппаратных и программных компонентов, составляющих Интернет;
– с точки зрения сетевой инфраструктуры, предоставляющей услуги распределенным Интернет-приложениям.

Интернет – это компьютерная сеть, которая объединяет сотни миллионов вычислительных устройств по всему миру. Не так давно эти вычислительные устройства были в основном традиционными настольными компьютерами, рабочими станциями Linux и так называемыми серверами, которые хранят и передают информацию, такую как веб-страницы и сообщения электронной почты. Однако все чаще к Интернету подключаются нетрадиционные интернет-системы, такие как ноутбуки, смартфоны, планшеты, телевизоры, игровые консоли, веб-камеры, автомобили, устройства экологического зондирования, фоторамки и домашние электрические системы и системы безопасности. Действительно, термин компьютерная сеть начинает звучать немного устаревшим, учитывая многие нетрадиционные устройства, которые подключаются к Интернету. В интернет-жаргоне все эти устройства называются **хостами** или **оконечными системами**. По состоянию на июль 2011г., было почти 850 миллионов конечных систем, подключенных к Интернету [ISC 2012], не считая смартфонов, ноутбуков и других устройств, которые только периодически подключаются к Интернету. В целом, по оценкам, более 2 миллиардов пользователей Интернета [МСЭ 2011].

Интернет (англ. Internet =internet work) - составная сеть или интерсеть, которая строится на основе физических сетей
– локальных - Local Area Networks (LAN) - сети компьютеров на небольших территориях (в радиусе не более 1-2 км);
– глобальных - Wide Area Networks (WAN) - объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах;
– городских (или сети мегаполисов) - Metropolitan Area Networks (MAN) -предназначены для обслуживания территории крупного города - мегаполиса.

Сети, входящие в составную сеть, называются **подсетями** (subnet), составляющими сетями или просто сетями. Компонентами составной сети могут являться как локальные, так и глобальные сети. Все узлы в пределах одной подсети взаимодействуют, используя единую для них технологию.

**Структура сети** состоит из узлов и магистралей сети Интернет,

в сети Интернет существует несколько сервисов или служб (E-mail, USENET, TELNET, WWW, FTP и др.). Одним из первых сервисов является электронная почта E-mail, но в настоящее время большая часть трафика в Интернет приходится на службу World Wide Web (всемирная паутина), которая содержит миллионы страниц информации с различными видами документов.

Оконечные системы соединены между собой сетью **каналов связи** и **пакетных коммутаторов**. Существует множество типов каналов связи, которые состоят из различных типов физических носителей, включая коаксиальный кабель, медный провод, оптическое волокно и радиочастотный спектр. Различные каналы связи могут передавать данные с разной скоростью, **скорость передачи** измеряется в битах/секунду.

Когда одна оконечная система имеет данные для отправки в другую оконечную систему, отправляющая система сегментирует данные и добавляет байты заголовка к каждому сегменту. Полученные в результате пакеты информации, известные как **пакеты** на жаргоне компьютерных сетей, затем отправляются через сеть в оконечную систему назначения, где они собираются в исходные данные. На рис.1.4, заимствованном из учебника J.Kurose, K.Ross. Computer networking ATop-Down Approach, приведены составные части сети Интернет[7].

Пользователи подключаются к сети через маршрутизаторы местных поставщиков услуг Интернета или провайдеров ISP (см.рис.1.4), таких как местные кабельные или телефонные компании, корпоративные Интернет-провайдеры, университетские Интернет-провайдеры и Интернет-провайдеры, которые обеспечивают доступ WiFi в аэропортах, гостиницах, кафе и других общественных местах. Каждый провайдер сам является сетью пакетных коммутаторов и каналов связи. Интернет-провайдеры предоставляют различные типы сетевого доступа к конечным системам, включая широкополосный доступ (кабельный модем или DSL), высокоскоростной доступ к локальной сети, беспроводной доступ и 56 кбит/с коммутируемый модемный доступ. Интернет-провайдеры также предоставляют доступ в Интернет поставщикам Контента, подключая веб-сайты непосредственно к Интернету.

[7] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



Интернет - это подключение конечных систем друг к другу, поэтому Интернет-провайдеры, обеспечивающие доступ к конечным системам, также должны быть взаимосвязаны.

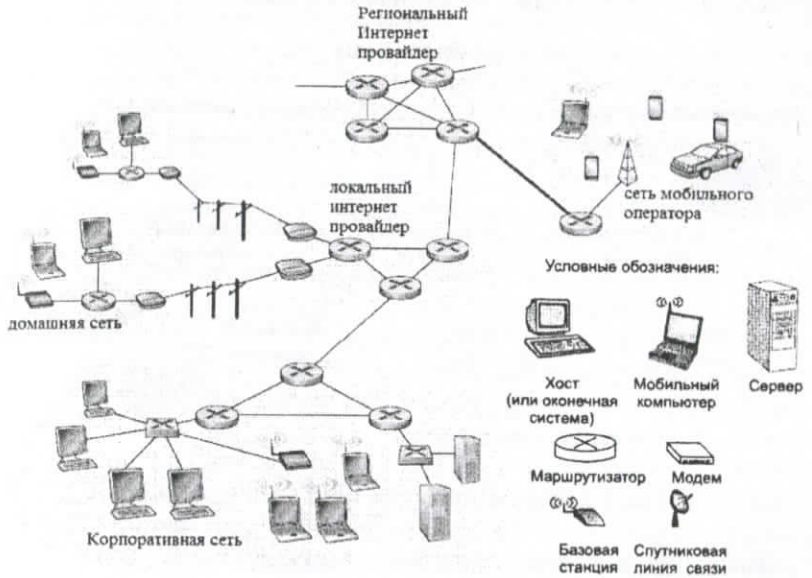



Рис.1.4. Составные части сети Интернет

Местные (локальные) Интернет-провайдеры имеют постоянное подключение к Интернет через региональных провайдеров. Региональный провайдер, подключается к более крупному провайдеру национального масштаба, имеющего узлы в различных городах страны.

Сети национальных провайдеров объединяются в сети транснациональных провайдеров или провайдеров первого уровня (см.рис.1.5). Объединенные сети провайдеров первого уровня составляют глобальную сеть Интернет.

Интернет-провайдеры нижнего уровня связаны между собой через национальных и международных Интернет-провайдеров верхнего уровня, таких как Level 3 Communications, AT&T, Sprint и NTT. Сеть интернет-провайдеров верхнего уровня состоит из высокоскоростных маршрутизаторов, соединенных высокоскоростными волоконно-оптическими линиями. Каждая сеть

интернет-провайдеров (ISP), будь то верхний или нижний уровень, управляется независимо, запускает IP-протокол и соответствует определенным соглашениям об именах и адресах.


Рис.1.5. Взаимодействие Интернет-провайдеров

Конечные системы, пакетные коммутаторы и другие части интернета запускают протоколы, которые контролируют отправку и получение информации в Интернете. TCP и IP протоколы являются двумя наиболее важными протоколами в Интернете. Протокол IP определяет формат пакетов, которые отправляются и принимаются между маршрутизаторами и конечными системами. Основные протоколы Интернета в совокупности называются TCP/IP.

Компоненты структуры сети Интернет объединяются в общую иерархию.

Интернет объединяет множество различных компьютерных сетей и отдельных компьютеров, которые обмениваются между собой информацией. Вся информация в Интернет хранится на Web-серверах. Обмен информацией между Web-серверами осуществляется по высокоскоростным магистралям.

Рассмотрев ответ на вопрос: «что такое Интернет и как построена сеть Интернет» с точки зрения основных аппаратных и программных компонентов, составляющих Интернет, попробуем описать Сеть под совершенно другим углом, а именно, как инфраструктуру, которая предоставляет услуги приложениям. Эти



приложения включают электронную почту, веб-серфинг, социальные сети, обмен мгновенными сообщениями, голосовую IP-телефонию (VoIP), потоковое видео, распространяемые игры, пиринговый обмен файлами (P2P), телевидение через Интернет, программы удаленного входа в систему, и многое, многое другое. Эти приложения точнее надо называть распределенными приложениями, так как они включают в себя несколько конечных систем, которые обмениваются данными друг с другом. Важно отметить, что Интернет-приложения работают на конечных системах – они не работают в пакетных коммутаторах в ядре сети. Хотя пакетные коммутаторы облегчают обмен данными между конечными системами, они не связаны с приложением, которое является источником или приемником данных.

Давайте рассмотрим, что подразумевается под инфраструктурой, которая предоставляет услуги приложениям. Предположим, что у вас есть новая захватывающая идея для распределенного Интернет-приложения, которое может принести большую пользу человечеству, или просто сделать вас богатым и знаменитым. Как вы могли бы превратить эту идею в реальное Интернет-приложение? Поскольку приложения выполняются в конечных системах, вам потребуется написать программы, которые выполняются в конечных системах. Можно, например, писать программы на Java, C или Python. Теперь, поскольку вы разрабатываете распределенное Интернет-приложение, программы, работающие на разных конечных системах, должны будут отправлять данные друг другу. И здесь мы переходим к центральному вопросу – вопросу, который приводит к альтернативному способу описания Интернета как платформы для приложений. Как одна программа, запущенная в одной конечной системе, предписывает Интернету доставлять данные в другую программу, работающую в другой конечной системе?

Конечные системы, подключенные к Интернету, предоставляют Интерфейс прикладного программирования (Application Programming Interface API), который определяет, как программа, работающая в одной конечной системе, запрашивает у инфраструктуры Интернета доставку данных в конкретную целевую программу, работающую в другой конечной системе. API интерфейс – это набор правил, которым должна следовать программа-отправитель, чтобы сеть Интернет могла доставить данные в программу-получатель. Рассмотрим простую аналогию, предположим, Алекс хочет отправить

письмо Дониёру с помощью почтовой службы. Алекс, конечно, не может просто написать письмо (данные) и выбросить письмо из окна. Вместо этого почтовая служба требует, чтобы Алекс положил письмо в конверт; написал полное имя Дониёра, адрес и почтовый индекс на конверте; запечатал конверт; и поместил конверт в почтовый ящик официальной почтовой службы или отнес его в почтовое отделение. Таким образом, почтовая служба имеет свой собственный "API почтовой службы" или набор правил, которым Алекс должен следовать, чтобы почтовая служба доставила свое письмо Дониёру. Аналогичным образом, сеть Интернет имеет API, которым программы-отправители данных должны следовать, чтобы сеть Интернет могла доставить данные в программу-получатель данных.

Почтовая служба, конечно же, предоставляет много услуг своим клиентам. Она обеспечивает экспресс-доставку, подтверждение регистрации, обычное использование и многие другие услуги. Аналогичным образом, Интернет предоставляет множество услуг для своих приложений. При разработке Интернет-приложения вы также должны выбрать один из сервисов интернета для своего приложения. Мы опишем услуги Интернета в главе 8.

## 1.4. Основные понятия и определения, используемые при работе в Интернет

Интернет – всемирная компьютерная сеть, связывающая в единое целое миллионы вычислительных устройств в разных уголках земного шара:

- настольные персональные компьютеры, серверы, PDA, телевизоры, мобильные компьютеры – хост системы или оконечные системы;
- **рабочая станция** — это компьютер, за которым непосредственно работает абонент компьютерной сети;
- **сервер** — это компьютер, выполняющий общие задачи компьютерной сети и предоставляющий услуги рабочим станциям.

**Хост** – это универсальная точка подключения к сети Интернет, имеющая IP-адрес. Это компьютер, который выполняет приложения и имеет одного или нескольких пользователей, поддерживающий протокол TCP/IP хост работает как конечная точка сетевой коммуникации.



**IP-адрес** имеет фиксированную длину 4 байта (32 бита). Распространенной формой представления IP-адреса является запись в виде **четырех чисел**, представляющих значения каждого байта в десятичной форме и разделенных точками, например: 128.10.2.30 . Этот же адрес может быть представлен в двоичном формате: 10000000 00001010 00000010 00011110

Максимальное количество IP-адресов в Сети $2^{32}$=4 294 967 296.

Человеку трудно запомнить числовой адрес, поэтому была введена доменная система имен (DNS), которая ставит в соответствие числовому Интернет - адресу уникальное доменное имя. Домен – это группа компьютеров, объединенных по некоторому признаку. Доменная система имен имеет иерархическую структуру: домены верхнего (первого) уровня; домены второго уровня; домены третьего уровня и т.д. (справа налево), как показано на рис.1.6.

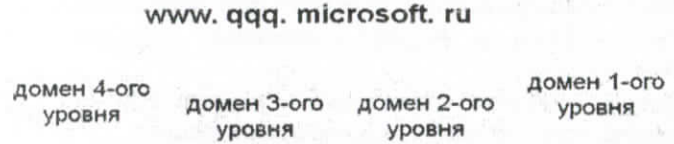



Рис.1.6. Пример доменной системы имен

Связь между хост системами осуществляется с помощью множества последовательных линий, соединяемых специальными коммутирующими устройствами – маршрутизаторами. Маршрутизатор принимает порцию данных, передаваемых по одному из его входных каналов связи и перенаправляет её в один из своих выходных каналов связи. Пакеты – передаваемые порции данных. Последовательность каналов связи и маршрутизаторов, через которые проходит пакет – маршрут или путь пакета в сети. Путь пакета заранее неизвестен и определяется непосредственно в процессе передачи

Доступ оконечных систем к Интернет через поставщиков услуг Интернета или Интернет-провайдеров. Интернет-провайдер выполняет следующие функции:

- предоставляет сеть маршрутизаторов и линий связи и предлагают способы подключения оконечных систем к сети

различными способами – Dial-up, широкополосное подключение при помощи цифровой АЛ, высокоскоростной доступ через локальную сеть, беспроводный доступ;
– прямое подключение к сети web-сайтов.

Магистральные операторы имеют магистральные каналы связи на крупной территории (страна, континент). Региональные операторы предоставляют услуги в одном региона (область, край, штат). Локальные операторы предоставляют услуги в пределах города.

Каждый Интернет-провайдер является административной единицей, передающей данные по протоколу IP и придерживающейся соглашений об именах и адресах, принятых в Интернете. Хосты, маршрутизаторы и др. компоненты Интернета используют протоколы для управления приёмом и передачей информации внутри Сети.

**Протокол** – набор правил передачи информации в сети, которых должны придерживаться все компании, чтобы обеспечить совместимость аппаратного и программного обеспечения. Протокол определяет – типы и формат сообщений, порядок следования сообщений.

Сетевой протокол аналогичен человеческому протоколу, за исключением того, что объекты, обменивающиеся сообщениями и выполняющие действия, являются аппаратными или программными компонентами какого-либо устройства (например, компьютера, смартфона, планшета, маршрутизатора или другого устройства с поддержкой сети). Вся деятельность в Интернете, которая включает в себя два или более взаимодействующих удаленных объектов регулируется протоколом. Например, аппаратно реализованные протоколы на двух физически подключенных компьютерах управляют потоком битов на «шинах» между двумя сетевыми интерфейсными картами; протоколы управления перегрузкой в конечных системах контролируют скорость, с которой пакеты передаются между отправителем и получателем; протоколы в маршрутизаторах определяют путь пакета от источника до назначения. Протоколы работают везде в Интернете, и, следовательно, большая часть этой книги посвящена сетевым протоколам компьютера.

В качестве примера протокола компьютерной сети, с которым вы, вероятно, знакомы, рассмотрим, что происходит, когда вы делаете запрос к веб-серверу, то есть, когда вы вводите URL веб-страницы в веб-браузере. Сценарий показан на рис.1.7. Сначала



компьютер отправит на веб-сервер сообщение с запросом на подключение и будет ждать ответа. Веб-сервер в конечном итоге получит сообщение с запросом на подключение и вернет ответное сообщение на подключение. Зная, что теперь можно запросить веб-документ, ваш компьютер затем отправляет имя веб-страницы, которую он хочет получить от этого веб-сервера в сообщении GET. Наконец, Веб-сервер возвращает веб-страницу (файл) на ваш компьютер. Учитывая приведенные выше человеческие и сетевые примеры, обмен сообщениями и действия, предпринятые при отправке и получении этих Сообщений, являются ключевыми определяющими элементами протокола.

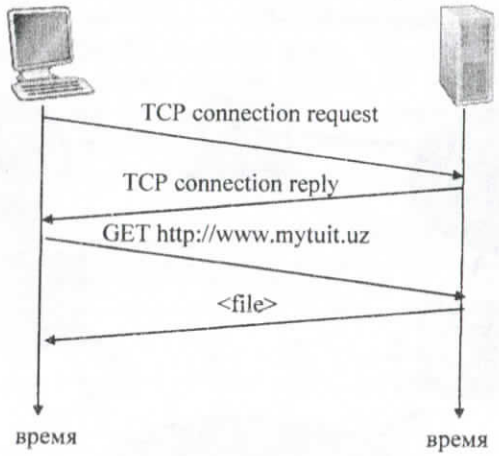



Рис.1.7. Пример работы протокола компьютерной сети

Протокол определяет формат и порядок обмена сообщениями между двумя или более взаимодействующими объектами, а также действия, предпринятые в отношении передачи и/или получения сообщения или другого события.

Интернет и компьютерные сети широко используют протоколы. для выполнения различных задач связи используются различные протоколы. Сеть Интернет объединяет сети, работающие по разным **правилам** (протоколам). Для согласования правил используют специальные компьютеры, которые называются **шлюзы** (см.рис.1.8).

В сети Интернет существует 2 типа протоколов – базовый и прикладные. Базовые протоколы (TCP/IP) отвечают за физическую пересылку данных по Сети. Прикладные – отвечают за работу специализированных служб, например (http – протокол передачи гипертекстовых сообщений, ftp – протокол передачи файлов).

В среде клиент/сервер Интернет на базе TCP/IP, сервер назначает порты с учётом протокола прикладного уровня, который выполняется на клиентском уровне. Номер порта – это 16-битовые величины в диапазоне от 0 до 65 536. Общеизвестные порты используются системными процессами или прикладными программами, нумеруются числами из диапазона от 0 до 1 023. Например, порт 25 - протокол SMTP (Простого протокола пересылки почты), порт 80 - протокола HTTP.

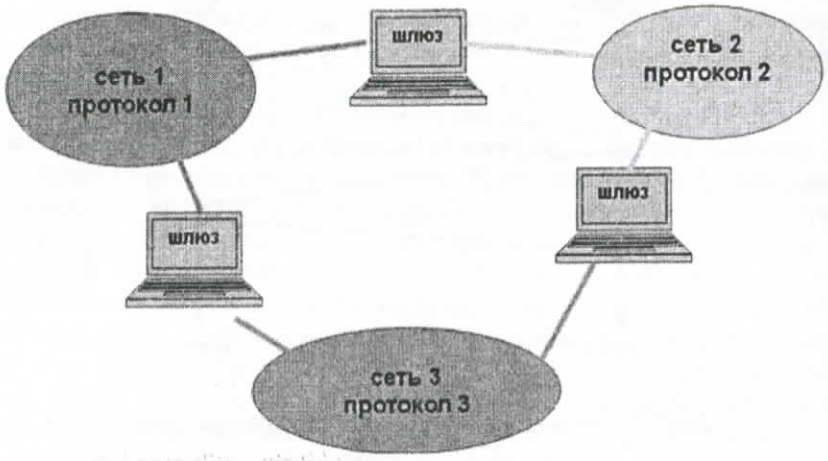



Рис.1.8. Местоположение и функции

У каждого Web-документа (и даже у каждого объекта, встроенного в такой документ) в Интернете есть свой *уникальный адрес* — он называется унифицированным указателем ресурса URL (Uniformed Resource Locator) или, сокращенно, **URL-адресом** (см.рис.1.9).



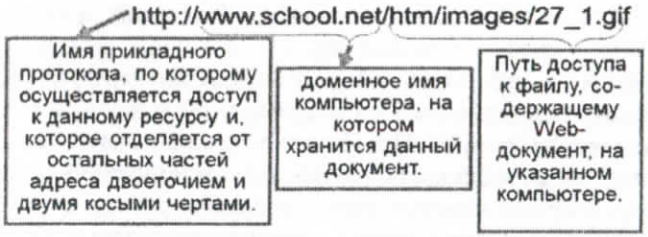



Рис.1.9. Структура URL-адреса

Браузер (browser) – (от анг. глагола to browse - просматривать, пролистывать) программа для просмотра страниц Интернета, точнее, Всемирной паутины (см.рис.1.10).

Узнет (Узнет = uz + net) — узбекистанская часть сети Интернет. В Узнете распространён русский язык, что позволяет «частично включать» Узнет в Рунет. Среди сайтов на узбекском языке — Узбекская Википедия. Часто под Узнетом понимается сеть обмена трафиком Tas-IX, так как у многих провайдеров доступ к ресурсам внутри Tas-IX является бесплатным для их абонентов.


Рис.1.10. Пример Браузера (browser)

Русскоязычная часть сети Интернет называется Рунéт (Рунет = ru + net). вошло в употребление стихийно во второй половине 1990г.г., его происхождение точно не известно. Одно из толкований, ru - доменное имя + net – от англ. слова network (net) «сеть».

## 1.5. Стандарты в сфере Интернет

Интернет - самая необычная из всех сетей. Практически любой объект может подключиться к Интернет, чтобы предложить ресурсы, или для доступа к ним. По Интернет может гулять практически любой вид информации без каких-либо ограничений. Отсутствует центральный орган, который регулировал бы работу сети Интернет, хотя существуют организации, устанавливающие определённые фундаментальные принципы и руководящие работой сети. Сеть Интернет по своей философии является автономной и даже анархической; в конечном счёте, в этом и её сила, и её слабость.

Существует ряд организаций, которые участвуют в различных мероприятиях по администрированию и поддержке Интернет. В контексте данной книги среди этих организаций следует упомянуть CERT, IAB, IETF, IESG, IRTF, ICANN и The Internet Society (Общество Интернет, известное также как ISOC).

*Группа реагирования на нарушения компьютерной защиты (CERT)* - группа экспертов Университета Карнеги-Меллона, которая отвечает за вопросы, связанные с нарушением компьютерной защиты в сети Интернет. CERT была образована ARPA в ноябре 1998 года как реакция на ряд инцидентов, связанных с появлением вирусных программ самотиражирования.

*Совет по архитектуре Интернет (IAB),* первоначально – *Координационный совет сети Интернет* - добровольный орган, имеющий в своем составе 12 экспертов, которые используют ресурсы своих компаний-спонсоров для того, чтобы способствовать интересам Интернет. IAB контролирует и координирует деятельность двух проблемных (рабочих) групп: IETF и IRTF. В совокупности, эти организации вырабатывают техническую политику и направления работы.

*Инженерная проблемная группа Интернет (IETF)* определяет, устанавливает приоритеты и вырабатывает решения по краткосрочным вопросам и проблемам, включая протоколы, архитектуру и эксплуатацию. Предложенные стандарты публикуются в Интернет в виде Запросов комментариев и предложений (RFC). После выработки окончательной версии стандарта, он поступает на утверждение в *группу управления инженеров Интернет (IESG).*

*Научно-исследовательская проблемная группа Интернет (IRTF)* занимается долгосрочными вопросами, включая схемы адресации и технологии.



*Корпорация Интернет по присвоению имен и номеров (ICANN)* - некоммерческая организация, образованная в 1999 году. ICANN была создана для того, чтобы взять на себя полномочия федерального органа IANA по распределению общеизвестных номеров портов, управлению IP-адресами и присвоению имён доменов. Номера портов представляют собой 16-битовые величины в диапазоне от 0 до 65 536. Общеизвестные порты нумеруются числами из диапазона от 0 до 1 023 и используются системными процессами или прикладными программами. Примерами общеизвестных портов являются: порт 25 для протокола SMTP (Простого протокола пересылки почты), порт 80 для протокола HTTP (Гипертекстового транспортного протокола) и порт 107 для Дистанционной службы Telnet. В среде клиент/сервер Интернет на базе протокола TCP/IP, сервер назначает порты с учётом протокола прикладного уровня, который выполняется на клиентском уровне. ICANN также присваивает IP-адреса организациям, желающим поместить компьютеры в Интернет; количество адресов зависит от размера организации.

*Общество Интернет (ISOC)* -добровольная организация, которая представляет собой некоторую формальную структуру для администрирования Интернет. Общество Интернет предоставило официальные полномочия IESG принимать решения по стандартам.

## 1.6. Обобщённая структура телекоммуникационной сети с точки зрения сети Интернет

### 1.6.1. Понятие о системах электросвязи

**Информация** – это сведения, являющиеся объектом хранения, передачи, преобразования. **Сообщение** — это форма выражения (представления) информации, удобная для передачи на расстояние. Объем сообщения, определяется всей указанной информацией и чаще всего оценивается числом знаков (букв или цифр) или временем его передачи, когда речь идет о телефонных сообщениях или вещании программ. Применительно к сфере телекоммуникаций сообщение – это информация, передаваемая с помощью электромагнитных сигналов средствами электросвязи.

По характеру изменения информационных параметров различают непрерывные и дискретные сообщения. Физический процесс, отображающий передаваемые сообщения, называют **сигналом**.

Процесс передачи или приема сигналов, знаков, текстов, изображений, звуков по проводной, радио, оптической или другим электромагнитным системам называется **электросвязью**. Классификация сетей электросвязи разнообразна, но в основном определяется видами передаваемых сообщений, средой распространения электрических сигналов и способами распределения информации: коммутируемы и некоммутируемые сети передачи сообщений.

Служба передача данных — вид связи, которая обеспечивает передачу дискретных сообщений в виде цифровых данных. Телефонная связь — вид связи, предназначенный для обмена информацией путем передачи звуковых сообщений (разговора) с использованием телефонных аппаратов. Звуковое вещание — вид связи, предназначенный для передачи программ звукового вещания широкому кругу территориально рассредоточенных слушателей посредством радио- и проводных линий. Телефонная связь обеспечивает ведение переговоров между людьми (абонентами), а звуковое вещание — одностороннюю и высококачественную передачу звуковых сообщений (радиопрограмм), предназначенных одновременно для многих слушателей. Телевизионное вещание осуществляют одновременную передачу оптических и звуковых сообщений, обеспечивая одновременную передачу сообщений для широких масс населения.

### 1.6.2. Обобщённая структура телекоммуникационной сети

Сеть связи — часть системы связи, представляющая собой совокупность узлов и линий связи, выделенная по определенному признаку (виду, роду связи, структурной и функциональной автономности и др.) и предназначенная для обмена информацией между абонентами (пользователями) связи. Сеть телекоммуникаций – совокупность оконечных устройств, коммутационных центров и связывающих их линий и каналов связи с единым управлением. Несмотря на сохраняющиеся различия между компьютерными, телефонными, телевизионными, радио-сетями, в их структуре можно найти много общего. В общем случае телекоммуникационная сеть состоит из (см.рис.1.11)[8]:

[8] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010



– терминального оборудования пользователей (возможно, объединенного в сеть);
– сетей доступа;
– магистральной сети;
– информационных центров, или центров управления сервисами (Services Control Point, SCP).


Рис.1.11. Структура телекоммуникационной сети

Сеть доступа - нижний уровень иерархии ТК сети. Основное назначение сети доступа — *концентрация информационных потоков,* поступающих по многочисленным каналам связи от оборудования клиентов к узлам магистральной сети.

Терминальное оборудование зависит от сети, в которой используется, например, компьютерная сеть - компьютеры, телефонная - телефонные аппараты, телевизионная – приемники телевизионного сигнала, радиосеть - радиоприемники. Терминальное

оборудование пользователей может быть объединено в сети, которые не включаются в состав ТК сети, т.к. принадлежат пользователям и размещаются на их территории. Компьютеры пользователей объединяются в локальные сети (local Area Network, LAN), а телефоны могут подключаться к **офисному телефонному коммутатору** (Private Branch Exchange, PBX).

Сеть доступа — это региональная сеть, отличающаяся большой разветвленностью. Как и ТК сеть в целом, может состоять из нескольких уровней (на рис. показано 2 уровня). Коммутаторы, установленные в узлах нижнего уровня, мультиплексируют информацию, поступающую по многочисленным абонентским каналам, часто называемым **абонентскими окончаниями,** и передают ее коммутаторам верхнего уровня. Коммутаторы верхнего уровня передают информацию коммутаторам магистрали. Количество уровней сети доступа зависит от ее размера: небольшая сеть доступа 1 уровень, крупная 2-3 уровня.

Магистральная сеть объединяет отдельные сети доступа, обеспечивая транзит трафика между ними по высокоскоростным каналам. Коммутаторы магистрали могут оперировать не только информационными соединениями между отдельными пользователями, но и агрегированными информационными потоками, переносящими данные большого количества пользовательских соединений. Информация с помощью магистрали попадает в сеть доступа получателей, где она демультиплексируется и коммутируется таким образом, чтобы на входной порт оборудования пользователя поступала только адресованная ему информация.

Информационные центры реализуют информационные услуги сети. Могут хранить информацию 2 типов:

- пользовательская информация
- вспомогательная служебная информация.

Пользовательская информация - информация, которая непосредственно интересует конечных пользователей сети:

- Интернет сеть – веб-порталы справочной информации, новостей, электронных магазинов
- телефонные сети – услуги экстренного вызова (милиция, скорая помощь), справочные услуги различных организаций и предприятий - вокзалов, аэропортов, магазинов и т.п.

Вспомогательная служебная информация - помогает поставщику услуг предоставлять услуги пользователям.



- системы аутентификации и авторизации пользователей - для проверки провайдером прав пользователей на получение тех или иных услуг;
- системы биллинга - считают в коммерческих сетях плату за полученные услуги;
- базы данных учетной информации пользователей - хранят имена и пароли, список услуг, на которые подписан каждый пользователь.

Отличия сетей от обобщенной структуры ТК сети зависят от назначения и размера сети. Например, небольшая LAN - нет ярко выраженных сетей доступа и магистрали; корпоративная сеть - отсутствует система биллинга, т.к. услуги сотрудником предприятия оказываются не на коммерческой основе; ТВ сеть - сеть доступа приобретает вид распределительной сети, информация распространяется только в одном направлении — из сети к абонентам.

### 1.6.3. Методы классификации компьютерных сетей

Компьютерные сети классифицируются по многим признакам. Основными признаками для классификации компьютерных сетей являются [9]:

- технологические характеристики сетей;
- организационные критерии;
- функциональная роль в составной сети.

С точки зрения технологических характеристик сети классифицируются по следующим признакам:

- территория покрытия
- тип среды передачи
- топология,
- метод коммутации,
- метод продвижения пакетов,
- первичные (транспортные) и наложенные сети.

По территории покрытия сети бывают:

- локальные - Local Area Networks (LAN) - сети компьютеров на небольших территориях (в радиусе не более 1-2 км)

[9] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010

– глобальные - Wide Area Networks (WAN) - объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах
– городские (или сети мегаполисов) - Metropolitan Area Networks (MAN) -предназначены для обслуживания территории крупного города - мегаполиса.

По типу среды передачи сети делятся на:

– проводные сети, то есть сети, каналы связи которых построены с использованием медных или оптических кабелей;
– беспроводные сети - для связи используются беспроводные каналы связи (радио, СВЧ, инфракрасные или лазерные каналы).

Тип среды передачи влияет скорость и надежность соединения, обеспечиваемого каналом, частоту искажения в нем битов информации. Любая беспроводная среда гораздо больше подвержена влиянию внешних помех, чем проводная. Роса, туман, солнечные бури, работающие в комнате микроволновые печи - источники помех, которые могут привести к резкому ухудшению качества беспроводного канала.

По методу коммутации различают сети:

- сети с коммутацией пакетов, которые делятся на
  - дейтаграммные сети (Ethernet);
  - сети, основанные на логических соединениях – IP-сети, использующие на транспортном уровне протокол TCP;
  - сети, основанные на виртуальных каналах (MPLS-сети).
- сети с коммутацией каналов – пример телефонные сети на основе канала 64кбит/с.

С точки зрения топологии различают сети полносвязной топологии, дерево, звезда; кольцо, смешанная топология [10]. На рис.1.12 приведены примеры наиболее часто используемых топологий.

Первичные (транспортные) сети – сети, которые создают постоянные физические двухточечные каналы для других компьютерных и телефонных сетей. В их состав входят кабели, коммуникационное оборудование, которое позволяет прокладывать новые физические каналы между конечными точками сети. На рис.1.13 показана транспортная телекоммуникационная сеть

[10] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010



Республики Узбекистан, которая обеспечивает передачу информации внутри государства. Транспортная магистральная международная сеть Узбекистан организована на базе волоконно-оптических линий связи ВОЛС, аренды спутниковой емкости спутниковых систем связи, цифровых радиорелейных линий связи и цифровых систем передачи ЦСП по медным кабелям. Как видно из рис.1.13 в областном центре каждой зоны установлены автоматические междугородние телефонные станции АМТС.

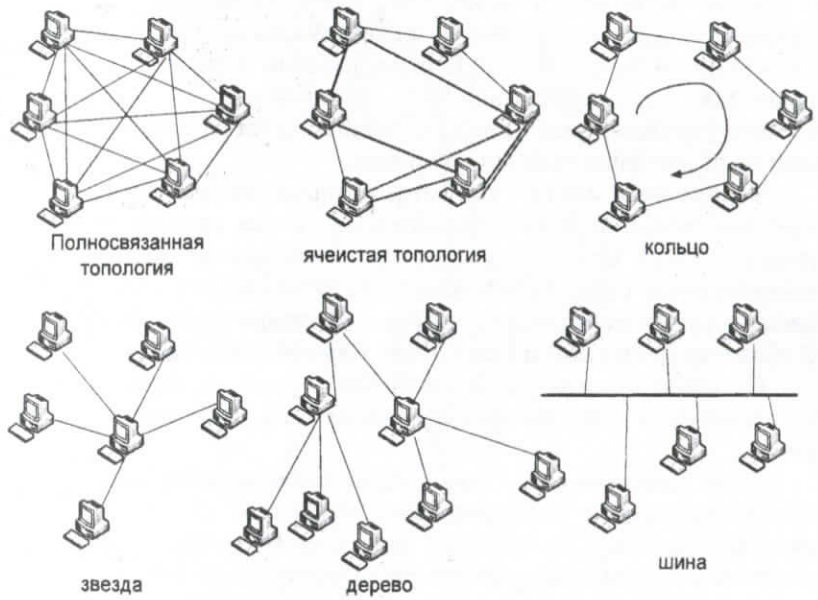



Рис.1.12. Топологии сетей

АМТС, установленные в городах Ташкент и Бухара, выполняют функции международных центров коммутации МЦК, которые обеспечивают пропуск междугородного и международного трафика. Четыре междугородных центра коммутации МГЦК (УАК), расположенные в городах Пахта, Бухара, Булунгур, Коканд. Для внешнего выхода на страны СНГ организовано пять «пограничных

узлов» ПСУ в городах Андижан, Денау, Бухара, Нукус, Пахта. Соответственно, каждый из них обеспечивает связь с Республиками Киргизстан, Таджикистан, Туркмения, Казахстан.

На рис.1.13 показано, что через территорию Узбекистана проходит международная телекоммуникационная магистраль – Транс-азиатско-Европейская волоконно-оптическая линия связи ТАЕ ВОЛС. В 1993г. телекоммуникационные компании девяти стран приступили к строительству ТАЕ ВОЛС. Общая длина магистрали 22,7 тыс.км. ТАЕ ВОЛС соединила 20 стран, от Германии (Франкфурт-на-Майне) до Китая (Шанхай), и проходит через Казахстан, Узбекистан, Туркменистан, Иран, Турцию, Румынию, Украину, Польшу, Венгрию и Австрию. В окт.1998г. ТАЕ была введена в эксплуатацию. Она проложена параллельно крупнейшим российским телекоммуникационным сетям и непосредственно конкурирует с ними на рынке евроазиатского транзита.

Наложенные сети – это сети, которые предоставляют услуги конечным пользователям и строятся на основе каналов первичных (транспортных) сетей. Различают компьютерные, телефонные, и телевизионные сети. Телефонная сеть Узбекистана состоит из 13 телекоммуникационных зон, которые географически соответствуют 12 областям (вилоятам) и Республике Каракалпакистан.

С точки зрения функциональная роли в составной сети различают сети доступа, магистральные сети, сети агрегированного трафика.

Сети доступа — это сети, предоставляющие доступ индивидуальным и корпоративным абонентам от их помещений (квартир, офисов) до первого помещения (пункта присутствия) оператора сети связи или оператора корпоративной сети, отвечают за расширение глобальной сети до помещений ее клиентов. Магистральные сети — наиболее скоростная часть (ядро) глобальной сети, которая объединяет сети доступа в единую сеть. На рис.1.14 показано ядро сети на примере города Ташкента.

Сети агрегирования трафика — это сети, агрегирующие (собирающие) данные от сетей доступа для компактной передачи их по небольшому числу каналов связи в магистраль.



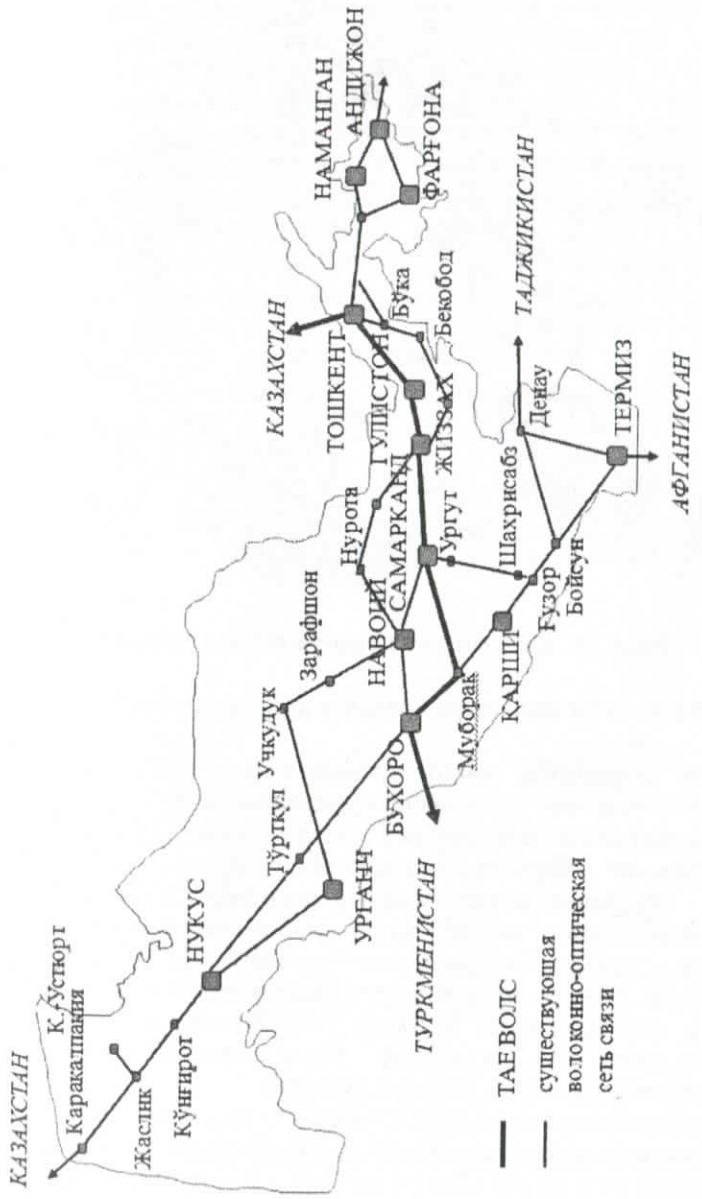



Рис.1.13. Транспортная телекоммуникационная сеть Республики Узбекистан

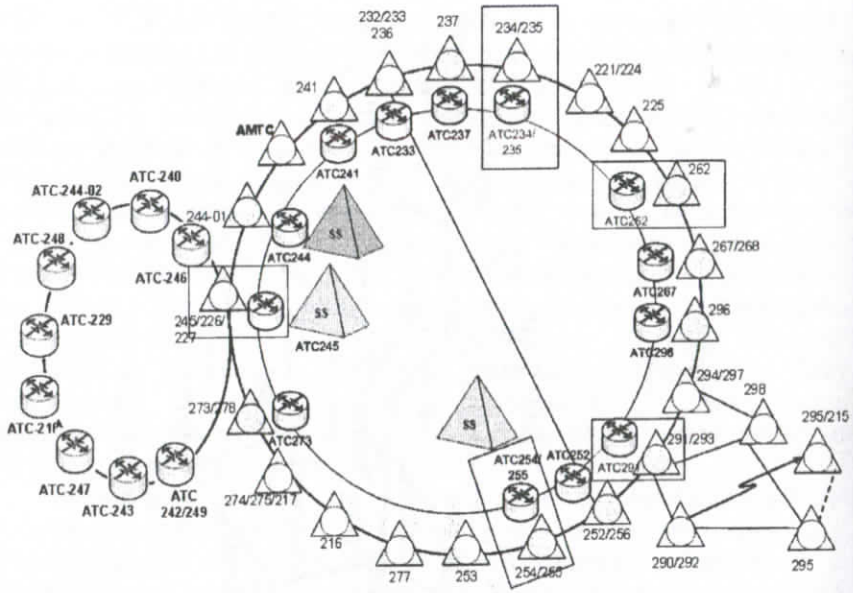



Рис.1.14. Ядро сети на примере города Ташкента

### 1.6.4. Сети операторов связи и корпоративные сети

Сети операторов связи предоставляют публичные услуги, клиентом сети может стать любой индивидуальный пользователь или любая организация, которая заключила коммерческий договор на предоставление телекоммуникационные услуги. Традиционные услуги - телефония, аренда каналов связи организациям, которые собираются строить на их основе собственные сети, доступ в Интернет, услуги виртуальных частных сетей, веб-хостинг, электронная почта, IP-телефония, широковещательная рассылка аудио- и видеосигналов. В такой сети больше клиентов, чем в корпоративной сети. Оператор несет прямую материальную ответственность за сбои в работе своей сети.

Корпоративные сети предоставляют услуги только сотрудникам предприятия, которое владеет этой сетью. Корпоративная сеть может иметь любой размер, это обычно сеть крупного предприятия, которая состоит из локальных сетей и из объединяющей их глобальной сети.



Различают 3 вида корпоративных сетей – сети отделов, сеть здания или сеть кампуса, сети масштаба предприятия.

Сети отделов – это сети, которые используются сравнительно небольшой группой сотрудников, работающих в одном отделе предприятия для решения общих задач (бухучет, маркетинг). В них обычно не более 30 пользователей, назначение такой сети совместное использование локальных ресурсов – приложений, данных, лазерных принтеров и модемов (см.рис.1.15)[11].

**Сеть здания** объединяет сети различных отделов одного предприятия в пределах отдельного здания, **сеть кампуса** - одной территории (кампуса), покрывающей площадь в несколько кв.км. Эти сети строятся по иерархическому принципу с собственной магистралью (см.рис.1.16)[12].

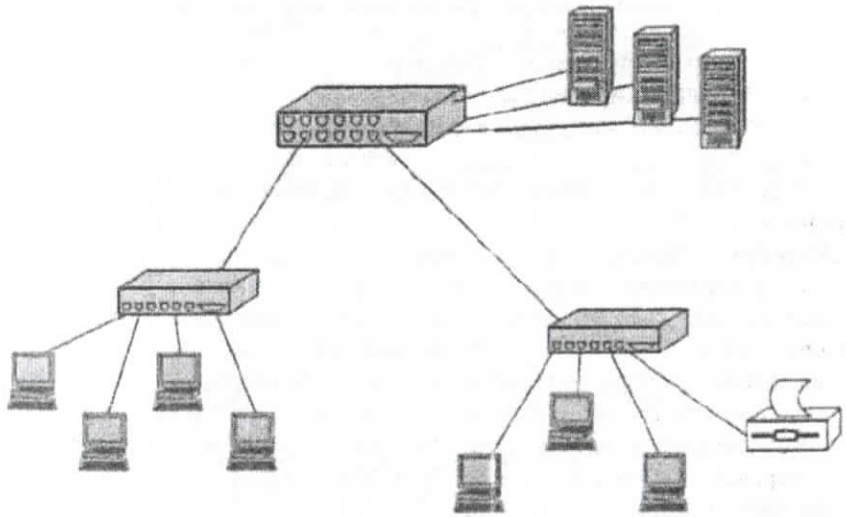


Рис.1.15. Сеть отделов

[11] В.Олифер, Н.Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010

[12] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010

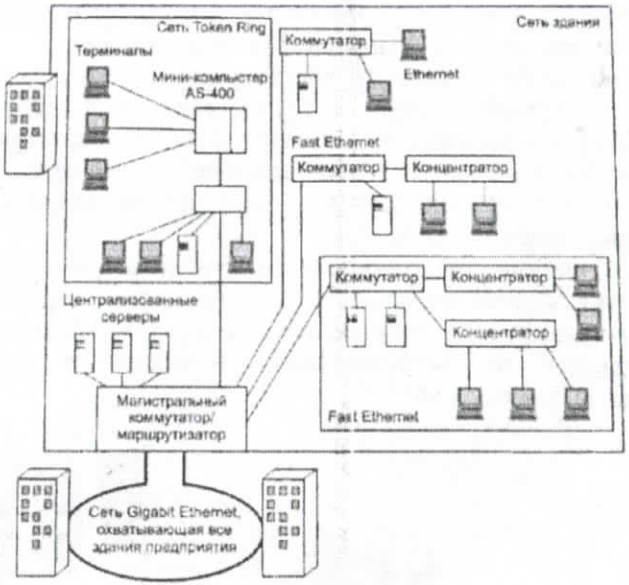



Рис.1.16. Сеть здания, кампуса

Главная задача сети масштаба предприятия оказание *информационных услуг.* Сети операторов связи могут и не предоставлять информационных услуг, так как компьютеры пользователей находятся за пределами зоны их ответственности. Сеть масштаба предприятия является примером инфокоммуникационной сети, она состоит из «островков» локальных сетей в ТК среде. Число пользователей и компьютеров может измеряться тысячами, число серверов — сотнями; Её отличительными характеристиками являются:

большие расстояния. Для соединения удаленных LAN и отдельных компьютеров применяются разнообразные ТК средства – в том числе каналы первичных сетей, радиоканалы, спутниковая связь.

- высокая степень неоднородности (гетерогенности) - различные типы компьютеров (от мэйнфреймов до персональных компьютеров), несколько типов ОС и множество различных приложений.



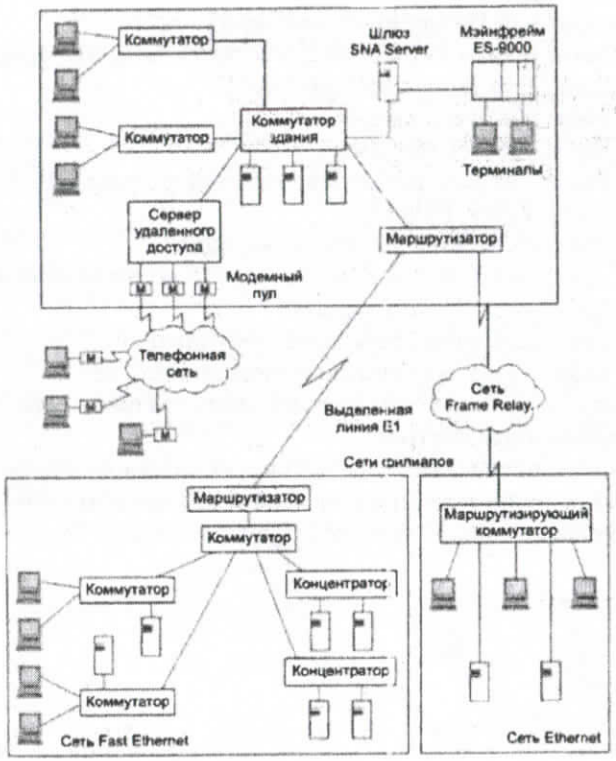



Рис.1.17. Сеть масштаба предприятия

## Контрольные вопросы

1. Что составляет основу структуры Интернет?
2. В чём разница между хостами и оконечными системами?
3. Что такое абонент, сервер, клиент?
4. Что такое подсеть (subnet)?
5. Что такое IP-адрес? Каково максимальное количество IP-адресов?
6. Что такое доменная система имен (DNS)?
7. Какие функции выполняет модем, маршрутизатор?
8. Что такое пакет, маршрут?
9. Что такое Интернет-провайдер?

10. Какие функции выполняют местный, национальный, международный Интернет-провайдеры?
11. Что такое протокол ? Какие существуют типы Интернет протоколов? Что такое порт протокола?
12. Что такое Интернет шлюз?
13. Что такое Браузер (browser )?
14. Что такое Унифицированный указатель ресурса URL?
15. Что такое Узнет, Рунет?
16. Что означает термин телекоммуникация?
17. Классификация систем электросвязи? Каково назначение различных системы электросвязи?
18. Что такое сеть связи, сеть телекоммуникаций?
19. Что входит в состав телекоммуникационной сети?
20. Каково назначение сети доступа, магистральной сети, информационных центров?
21. По каким признакам классифицируются компьютерные сети?
22. В чём отличие сети оператора связи от корпоративной сети?
23. Какие виды корпоративных сетей вы знаете?



# 2. СПОСОБЫ ПОДКЛЮЧЕНИЯ К ИНТЕРНЕТ

## 2.1. Виды сетей доступа

Сети доступа — это сети, предоставляющие доступ индивидуальным и корпоративным абонентам от их помещений (квартир, офисов) до первого помещения (пункта присутствия) оператора сети связи или оператора корпоративной сети, они отвечают за расширение глобальной сети до помещений ее клиентов.

Доступ к сети – это физическая линия связи, соединяющая оконечную систему с периферийным маршрутизатором – первым маршрутизатором на любом пути, исходящем из оконечной системы.

Существует 3 способа доступа к сети Интернет (см.рис.2.1)[13]:

- резидентный доступ - доступ рассредоточенных пользователей (Home Access) – подключение к сети домашних оконечных систем;
- корпоративный доступ – подключение к сети частных и государственных организаций;
- мобильный доступ – подключение портативных систем.

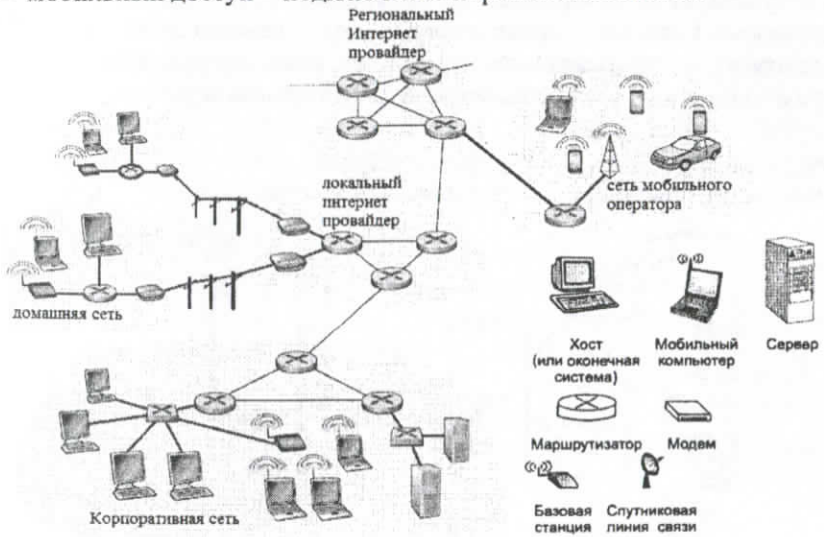



Рис.2.1. Способы подключения к Интернет - доступ к сети

[13] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

коммутируемый доступ по цифровой телефонной сети ISDN (цифровая сеть связи с интеграцией услуг) или с помощью беспроводных технологий: мобильный GPRS – Интернет и мобильный CDMA - Internet. На рис.2.3 приведен способ организации Dial-up доступа.


Рис.2.3. Способ организации Dial-up доступа

Модем преобразует цифровые сигналы компьютера в аналоговые сигналы, которые передаются через телефонный кабель. Сигнал принимается стороной интернет провайдера, групповой модем выполняет обратное преобразование. Максимальная скорость передачи данных Dial-up доступа 56кбит/с. Этого достаточно для доступа в Интернет, однако насыщение страниц графикой и видео, большие объемы электронной почты и документов в ближайшее время снова поставит вопрос о путях дальнейшего увеличения пропускной способности. Например, музыкальный файл длительностью 3мин формата MP3 будет загружаться 8мин. Более высокие скорости обеспечивает широкополосный доступ.

## 2.3. Доступ xDSL

На рис.2.4 приведен способ организации xDSL доступа. ADSL модемы размещаются на каждом конце абонентской линии клиента. Чтобы получить наибольшую ширину полосы частот в медной паре, технология ADSL - модема должна иметь алгоритмы, которые могут делить частотный диапазон приблизительно от 0.4МГц до 1.1МГц. Сплиттер – низкочастотный фильтр для присоединения ADSL модема к телефонным проводам, который не пропускает сигналы свыше заданной частоты. Поскольку при телефонном соединении все речевые сигналы меньше 4кГц , микрофильтры сформированы (LP –



Low Pass) так, чтобы блокировать все частоты выше 4кГц, препятствуя сигналам, переносящим данные, влиять на стандартные телефонные каналы. Даже если ADSL оборудование на данной абонентской линии повреждено, низкочастотный фильтр гарантирует непрерывное обслуживание телефонных вызовов.

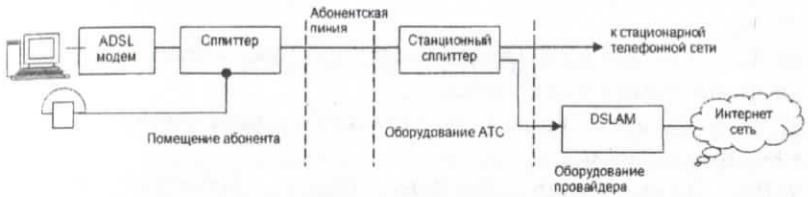



Рис.2.4. Способ организации xDSL доступа

На стороне АТС устанавливается DSLAM, который имеет следующие функции:

- создание широкополосных цифровых систем уплотнения шлейфа.
- частотная модуляция к удаленному модему цифровой АЛ, маршрутизация нагрузки передачи данных потоков "сеть - пользователь" и "пользователь - сеть".
- преобразования физического уровня.

Интернет-провайдер, местный узел используют DSLAM, чтобы соединить со станцией xDSL от квартирных абонентов и предприятий коммерческой деятельности. DSLAM должен принять данные исходящие от сотен модемов цифровой АЛ потока «сеть-пользователь», далее соединяя и мультиплексируя эти данные, вводя в частотные устройства для передачи на более высокой скорости. DSLAM объединяет поток «пользователь-сеть» со следующим устройством сети поставщика.

Доступ xDSL имеет следующие преимущества:

- использование существующих АЛ;
- значительное увеличение скорости передачи данных по медной паре телефонных проводов без необходимости их модернизации;
- передача по единственной АЛ всего разнообразного трафика массового пользователя – от традиционного телефонного разговора до доступа в Интернет;
- скорость передачи данных от 32кбит/с до 50Мбит/с.

В состав семейства технологий xDSL входят следующие технологии:

- ADSL (Asymmetric Digital Subscriber Line - асимметричная цифровая абонентская линия),
- RADSL (Rate-Adaptive Digital Subscriber Line - цифровая абонентская линия с адаптацией скорости соединения),
- ISDL (ISDN Digital Subscriber Line - цифровая абонентская линия IDSN),
- HDSL (High Bit-Rate Digital Subscriber Line - высокоскоростная цифровая абонентская линия),
- SDSL (Symmetric Digital Subscriber Line - симметричная цифровая абонентская линия),
- VDSL (Very High Bit-Rate Digital Subscriber Line - сверхвысокоскоростная цифровая абонентская линия),
- G.Lite, являющаяся упрощенным вариантом технологии ADSL, и их вариации

Таблица 2.1.

Характеристики технологий xDSL

| DSL технология | Макс. скорость передачи (на конце пользователя) | Макс. скорость приёма (на конце пользователя) | Макс. расстояние | Число линий |
|---|---|---|---|---|
| ADSL | 800кбит/с | 8Мбит/с | 5 500 м | 1 |
| ADSL- Lite (G.Lite ) | 512кбит/с | 1,536Мбит/с | 5 500 м | 1 |
| RADSL | 1Мбит/с | 7Мбит/с | 5 500 м | 1 |
| HDSL | 1,54-2Мбит/с | 1,54-2Мбит/с | 3 650 м | 2 |
| HDSL2 | 1,54-2Мбит/с | 1,54-2Мбит/с | 3 650 м | 1 |
| SHDSL | 192кбит/с-2,3Мбит/с | 192кбит/с-2,3Мбит/с | 7 500 м | 1 |
| VDSL | 16Мбит/с | 52Мбит/с | 1 200 м | 1 |
| VDSL2 | 100Мбит/с | 100Мбит/с | 150 м | 1 |
| SDSL | 2,3Мбит/с | 2,3Мбит/с | 6 700 м | 1 |
| MSDSL | 2Мбит/с | 2Мбит/с | 8 800 м | 1 |
| IDSL | 144кбит/с | 144 кбит/с | 10 700 м | 1 |

В таблице 2.1. приведены характеристики технологий xDSL.



Большинство технологий xDSL преследует различные цели. Асимметричные множества xDSL обычно используются для связи в Интернет и обеспечивают цены, ориентированные на квартирный сектор. Симметричная xDSL востребована в коммерческом секторе и применяется там, где требуются рабочие характеристики, подобные специализированным каналам точка-точка, или для высокоскоростных служб.

## 2.4. Кабельный доступ HFC

Доступ HFC – Hybrid Fiber Coaxial Cable – использует для передачи линии кабельного телевидения (см.рис.2.5)[14]. Распределительное устройство осуществляет вещание через сеть, которая состоит из коаксиального кабеля и усилителей, к ней подключены сотни домов. Оптоволоконный кабель соединяет распределительное устройство с передатчиками, к которым с помощью коаксиального кабеля подключены пользователи (500-5000 абонентов). Для HFC у пользователя должен быть установлен кабельный модем. В странах СНГ HFC не используется.


Рис.2.5. Принцип организации доступ HFC

## 2.5. Доступ FTTx

Сценарии развертывания FTTx (Fiber To The "x") зависит от комбинации трёх параметров архитектуры FTTx:

- положение точки "x"

[14] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

– у абонента,
– между абонентом и помещением узла связи оператора (подъезд дома, уличный шкаф и др.)

- технология доставки данных в оптической сети агрегации/распределения до точки "x"
  – активный Ethernet или какая-либо из разновидностей PON;
  – технологии спектрального уплотнения (в частности, CWDM) для увеличения пропускной способности и/или уменьшения количества волокон.
- технология доступа после точки "x "
  – как правило, xDSL, Ethernet или DOCSIS по медному кабелю,
  – беспроводной доступ (Wi-Fi).

Группа технологий FTTx включает в себя несколько видов технологий (см.рис.2.6):

- FTTA (Fiber To The Apartment) – доведение оптического кабеля волокна до квартиры жилого дома;
- FTTB (Fiber To The Building) – доведение оптического кабеля волокна до здания в 100м от абонента;
- FTTC (Fiber To The Curb) – доведение оптического кабеля до места установки кабельного шкафа в 500м от абонента;
- FTTH (Fiber To The Home) – доведение оптического кабеля до жилого дома, т.е. волокно в квартиру/офис абонента;
- FTTO (Fiber To The Office) – доведение оптического кабеля до офиса;
- FTTN (Fiber To The Node) – доведение оптического кабеля волокно до узла в 1км от абонента.

На рис.2.7 показаны варианты оптического доступа с точки зрения размещения оборудования, когда оптический кабель проложен непосредственно:

- - до оборудования абонента (вариант FTTH, при котором осуществляется подключение терминала ONT в жилище у абонента),
- - до здания или многоквартирного жилого дома (вариант FTTB, при котором подключение осуществляется оптического блока ONU, являющимся коммутатором доступа, расположенный в подъезде или на чердаке многоквартирного дома),
- - до распределительного шкафа (вариант FTTC, при котором точкой доступа может являться любое оборудование мультисервисного доступа).



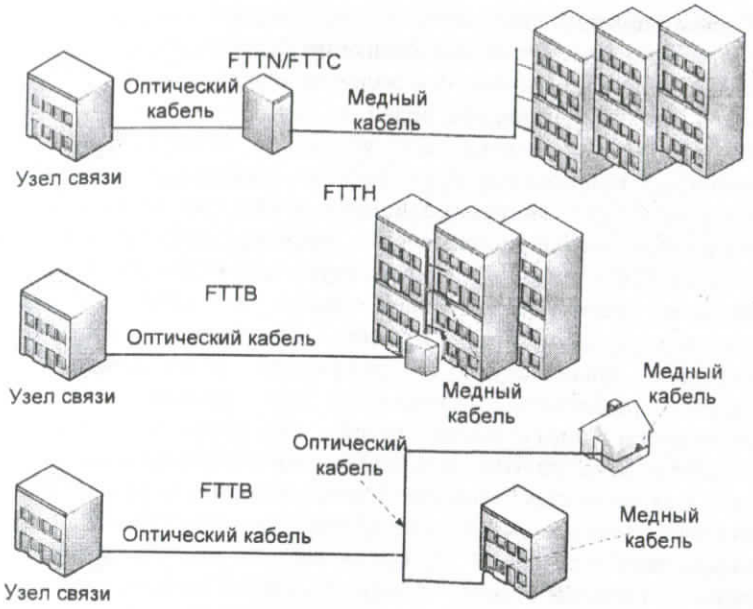



Рис.2.6. Варианты построения сетей FTTx с точки зрения абонентов

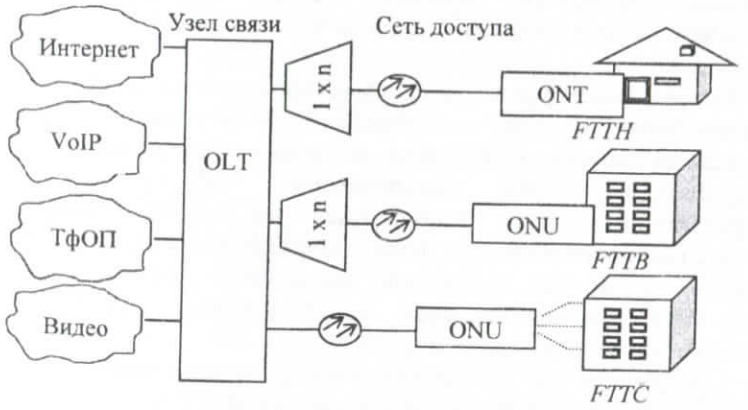



Рис.2.7. Варианты построения оптических сетей доступа с точки зрения размещения оборудования

Схемы организации оптического доступа характеризуются также применением оптических делителей (сплиттеров) (см. рис.2.7), позволяющих разделить емкость волокна между точками доступа с определенным коэффициентом деления (1xn).

В течение нескольких лет услуги, в которых нуждаются пользователи, приблизили предложение операторов вплотную к границе в 100Мбит/с. Использовавшиеся до сих пор технологии DSL-доступа не в состоянии удовлетворить такие запросы.

Сеть FTTB имеет трехуровневую логическую структуру. Выделенные логические уровни несут в себе следующую функциональную нагрузку. **Уровень Доступа (Access Layer)** осуществляет физическую концентрацию абонентских линий, организует разделение абонентов на уровне Ethernet с использованием виртуальных сетей, обеспечивает ограничение скорости передачи данных на входе в сеть и осуществляет базовые функции безопасности. **Уровень Распределения (Aggregation или Distribution Layer)** терминирует виртуальные сети Уровня Доступа с использованием протокола IP, предоставляет доступ к локальным ресурсам и позволяет вести обмен трафиком между различными узлами Уровня Распределения. **Уровень Ядра или уровень магистрали (Backbone или Core Layer)** служит высокоскоростной и надежной магистралью объединяющей Домены Распределения. Основной функцией данного уровня является передача пользовательского трафика с наибольшей скоростью и наименьшей задержкой.

Оборудование уровня доступа устанавливается в жилых домах, подключаемых к сети, и объединяется в кольца волоконно-оптическим кабелем (ВОК). Кольца уровня доступа замыкаются на оборудовании уровня распределения. Оборудование узлов распределения может располагаться на существующих узлах телекоммуникационной сети фиксированной или мобильной связи, а также на площадках, специально арендуемых для их размещения. Узлы Распределения, в свою очередь, также объединяются в кольцевые структуры с помощью ВОК.

При реализации технологии доступа архитектурой построения FTTB существует две схемы организации сети:

– древовидная топология организации сети,
– топология сети логическое объемное кольцо.

При реализации данной **древовидной топологии** оптический



кабель прокладывается от узлов агрегации до узлов распределения с помощью технологии пассивных оптических сетей (рис.2.8).

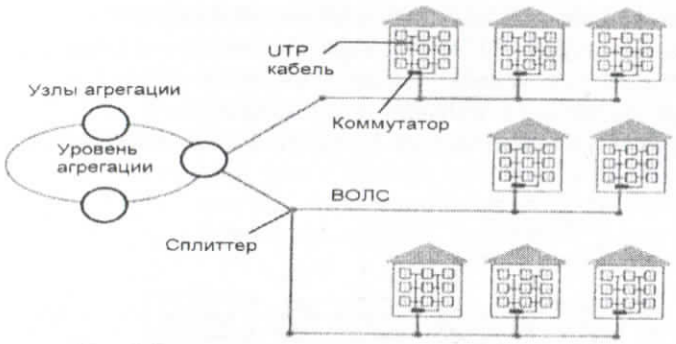



Рис.2.8. Древовидная схема организации FTTB

В **кольцевой топологии сети** оптический кабель прокладывается от узла агрегации к зданиям, например одного территориального района, по «цепочке», которая замыкается в другом узле агрегации (рис.2.9).


Рис.2.9. Схема организации FTTB топологией кольцо

В каждом доме (или на несколько домов) устанавливается коммутатор, включенный в кольцо по оптическому волокну, который соединяется с коммутаторами, устанавливаемыми внутри домов по витой паре. Коммутаторы устанавливаются в домовых и абонентских

ящиках. Подключение абонентов производится кабелем UTP-5. Прокладка кабелей внутри домов ведется либо по слаботочным щиткам, либо по собственной распределительной сети, построенной с применений пластиковых труб и абонентских ящиков.

Архитектура FTTC в первую очередь предназначена для операторов, уже использующих технологии xDSL или PON. FTTC подразумевает использование мультисервисного узла абонентского доступа MSAN (Multi Service Access Node) как показано на рис.2.10.

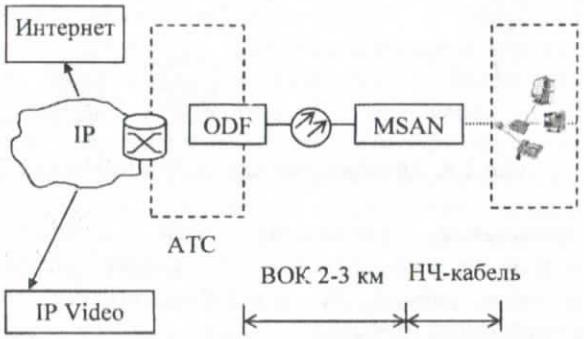



Рис.2.10. Развитие уровня доступа на базе MSAN

Из рисунка видно, что для реализации сети доступа по технологии FTTC необходимо следующее: оборудование – MSAN, маршрутизаторы/коммутаторы уровня агрегации, коммутаторы уровня доступа, оптический кросс ODF (Optical Distribution Frame).

При реализации MSAN на уровне доступа оптическая широкополосная сеть также будет иметь типичную двухуровневую структуру (OLT+ONU). В оборудование OLT будет подключаться MSAN. OLT – терминал (окончание) оптической линии, находится на станции и выполняет обработку протоколов, транспортировку и распределение потоков информации. ONU (Optical Network Unit) – оптический сетевой блок находится на стороне сети доступа и служит для предоставления абонентам доступа к сети. OLT управляет ONU. OLT может иметь доступ к нескольким ONU.

В случае многоэтажных построек с достаточно большим числом пользователей интернет выгодно подключать узлы доступа по кольцевой схеме с резервированием оптического волокна (рис.2.10).



Узлы доступа MSAN расположены в центре жилого массива в уличных шкафах. Между оборудованием уровня агрегации и уровня доступа используются две пары оптических волокон (прием и передача). На рис.2.11 приведена древовидная схема подключения MSAN. Надежность данной схемы ниже, чем кольцевой.

Наибольшее распространение получил способ организации сети доступа FTTH – точка-многоточка (P2MP) на базе пассивной оптической сети (PON). Сеть PON реализует топологию «точка — много точек», позволяя по одному оптическому волокну предоставлять услуги доступа 64 пользователям. Для разделения оптического сигнала в PON используются пассивные разветвители (сплиттеры).

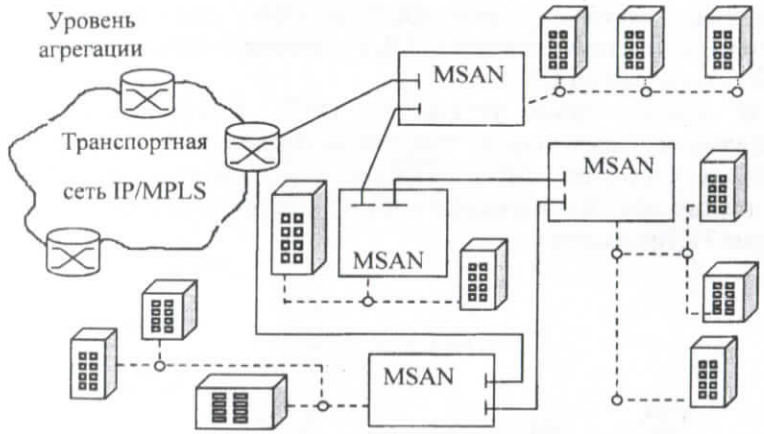



Рис.2.11. Вариант кольцевой схемы организации FTTC с MSAN

Архитектура FTTH на базе PON обычно поддерживает протокол Ethernet. В некоторых случаях используется дополнительная длина волны нисходящего потока (downstream), что позволяет предоставлять традиционные аналоговые и цифровые телевизионные услуги пользователям без применения телевизионных приставок с поддержкой IP.

При использовании архитектуры на базе пассивной оптической сети PON для развертывания сетей FTTH оптоволоконная линия распределяется по абонентам с помощью пассивных оптических

разветвителей с коэффициентом разветвления до 1:64 или даже 1:128. Архитектура FTTH на базе PON обычно поддерживает протокол Ethernet. В некоторых случаях используется дополнительная длина волны нисходящего потока (downstream), что позволяет предоставлять традиционные аналоговые и цифровые телевизионные услуги пользователям без применения телевизионных приставок с поддержкой IP.

На рис.2.12 показан принцип организации доступа в интернет по технологии FTTH[15]. OLT - optical line terminal - Терминал (окончание) оптической линии находится на станции, выполняет обработку протоколов, транспортировку и распределение потоков информации услуг. ONU - optical network terminator - Оптический сетевой блок находится на стороне сети доступа и служит для предоставления абонентам доступа к сети. OLT и ONU соединяются через оптическую систему передачи, OLT управляет ONU,может иметь доступ к нескольким ONU.

В каждом доме установлен ONT, который соединяется специальным выделеным волоконно-оптическим кабелем к сплиттеру. Сплиттер комбинирует волокна от нескольких домов (до 100) в один общий оптический кабель, который соединятся OLT на стороне ТК провайдера.

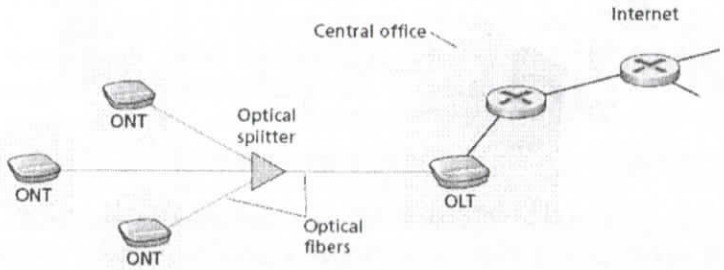



Рис.2.12. Доступ в интернет по FTTH

OLT предоставляет оптико/электрическое преобразование,

[15] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



подключается к интернет через маршрутизатор интернет-провайдера. Абоненты подключаются к домашнему маршрутизатору, который соединен с ONT, и получают доступ в интернет через домашний маршрутизатор. В архитектуре PON все пакеты, посылаемые от OLT через сплиттер, повторяются сплиттером.

### 2.6. Корпоративный доступ

Корпоративный доступ используется для подключения к сети интернет частных и государственных организаций, осуществляется при помощи технологии локальных сетей LAN, соединяющих оконечные системы с периферийным маршрутизатором (см.рис.2.13)[16].

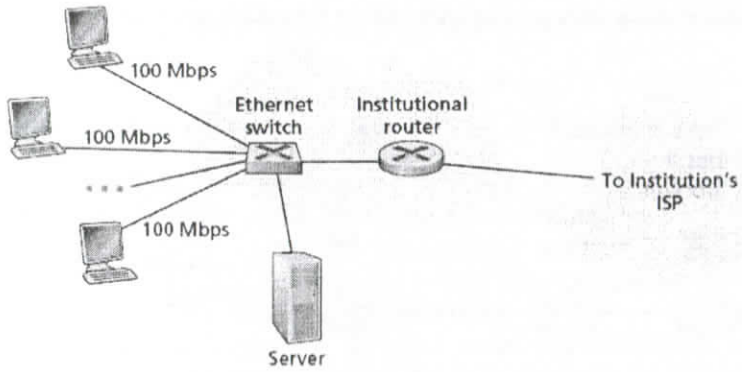



Рис.2.13. Корпоративный доступ в Сеть с использованием технологии Ethernet

### 2.7. Мобильный доступ

Существует два основных средства беспроводного подключения к сети интернет:

- беспроводные локальные сети WLAN,
- беспроводные сети удалённого доступа.

На рис.2.14 показан пример мобильного доступа на основе

[16] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

беспроводной локальной сети WLAN. Базовую станцию называют точкой беспроводного доступа[17]. Беспроводная локальная сеть WLAN обеспечивает дальность связи на десятки метров от точки беспроводного доступа. Базовая станция имеет прямое соединение с периферийным маршрутизатором Интернет с помощью ВОЛС.

Технологии доступа Wi-Fi и WiMax используются для получения беспроводного доступа к сети интернет, но решают разный круг задач. Как правило, Wi-Fi используют для построения беспроводных локальных сетей с радиусом действия в зависимости от окружающей среды от 50 и до 100 метров. В отличии от WiMax технология Wi-Fi интернет-провайдерами используется мало, но зато большую популярность этот вид беспроводного подключения к интернету получил в гостиницах, аэропортах, кафе, клубах, квартирах и домах. Потому что данная технология позволяет быстро, легко и удобно обеспечить всех желающих выйти в глобальную сеть.

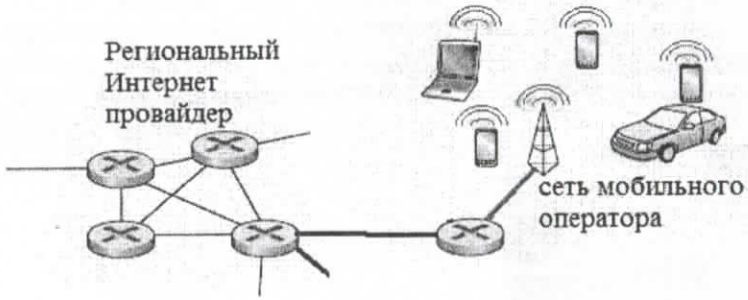



Рис.2.14. Мобильный доступ на основе беспроводной локальной сети WLAN

Технологии беспроводных сетей семейства 802.11b Wi-Fi (802.11b – Wireless Fidelity), которые обеспечивают передачу данных в диапазоне 2.4ГГц со скоростью 1, 2, 5,5 и 11Мбит/с. На рис.2.15 приведены способы организации WLAN 802.11b Wi-Fi.

Технологию WiMax для доступа в Интернет доступа используют там, где кабельный Интернет не доступен, в доме или в офисе нет выделенной сети или нет телефонной линии для ADSL подключения.

---

J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



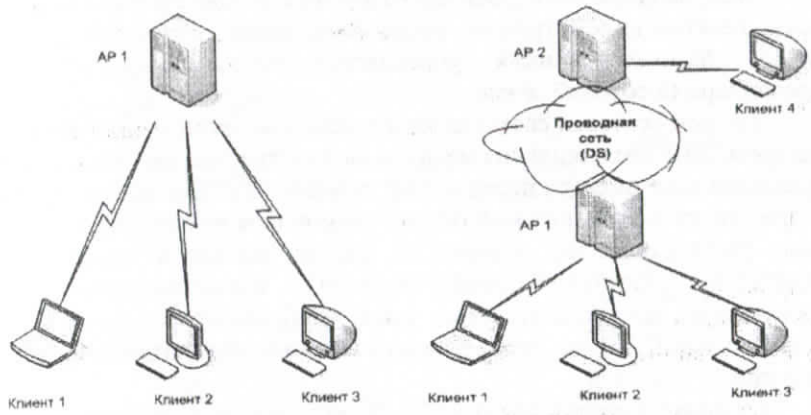



Рис.2.15. Способы организации WLAN 802.11b Wi-Fi

Технология WiMax теоретически имеет скорость передачи данных около 70Мбит/с, но на практике это скорость в разы меньше. Чтобы подключиться к Интернет нужно обратиться к предоставляющему провайдеру, который по карте покрытия сети определит, входит ли ваше место расположения в зону покрытия. Если выясниться, что место размещения клиента не попадает под зону покрытия, то специалистам нужно будет определить расстояние до ближайшей базовой станции к клиенту.

Желательно, что бы базовая станция находилась в прямой видимости от клиента, а расстояние составляло не более 10км. В зависимости от полученных результатов (расстояние и условие приема сигнала) потребуется подобрать WiMax модем и антенну с требуемым усилением. Кроме этого, потребуется кабель, чтобы соединить антенну с модемом и USB удлинитель для подключения модема с маршрутизатором или компьютером.

Антенну обычно устанавливают на максимально возможную точку и направляют (для расчета может использоваться программа Google Earth) ее как можно точнее на базовую станцию. После этого антенна соединяется с модемом, подключается к сети и подстраивается до максимального уровня сигнала. Очень часто для приема интернета по WiMax используют специализированный Wi-Fi маршрутизатор с USB-портом, который может работать WiMax модемом.

Беспроводные сети удалённого доступа обеспечивают дальность связи десятки километров от точки беспроводного доступа. В этом случае базовая станция управляется поставщиком услуг – провайдерами сотовой связи.

Термин «сотовая связь» связан с методом организации сети, при котором зона обслуживания делится на участки, называемые сотами. В каждой соте имеется передающая станция (BTS), которая передаёт и принимает сигналы от мобильных терминалов внутри соты. Размер соты (зона покрытия) зависит от многих факторов, таких как – мощность передатчика базовой станции BTS, мощность передатчиков абонентских устройств (сотовых телефонов), высота и расположение жилых зданий в сое, рельеф местности, высота антенны базовой станции.

Стандарт сотовой связи GSM 2G использует комбинированный FDM/TDM радио интерфейс для беспроводного доступа. Как будет описано в разделе 4.5, при частотном разделении каналов FDM рабочая полоса частот делится на некоторое количество диапазонов, называемых каналами, каждый из которых используется для одного вызова. При временном разделении каналов TDM цикл – периодически повторяющийся временной интервал делится на отдельные промежутки времени, называемые временными каналами (slot), каждый из которых используется для одного вызова. В комбинированном FDM/TDM радио интерфейсе рабочая полоса частот, делится на некоторое количество частотных поддиапазонов, каждый из которых разделяется на временные циклы и временные каналы (slot). Таким образом, в комбинированной FDM/TDM системе, если канал разделён на $F$ поддиапазонов, а каждый из них на $T$ временных каналов, то общий канал в состоянии обслужить $F \times T$ одновременных вызовов. Как мы видели в разделе 2.3, кабельные сети доступа также используют комбинированный FDM/TDM интерфейс, но в другом частотном диапазоне. Системы стандарта GSM используют диапазоны частот по 200кГц, каждый из которых поддерживает 8 TDM вызовов. Скорость кодирования речи стандарта GSM 12,2кбит/с, 13кбит/с. На рис.2.16 приведены компоненты сети сотовой связи 2G стандарта GSM[18].

[18] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



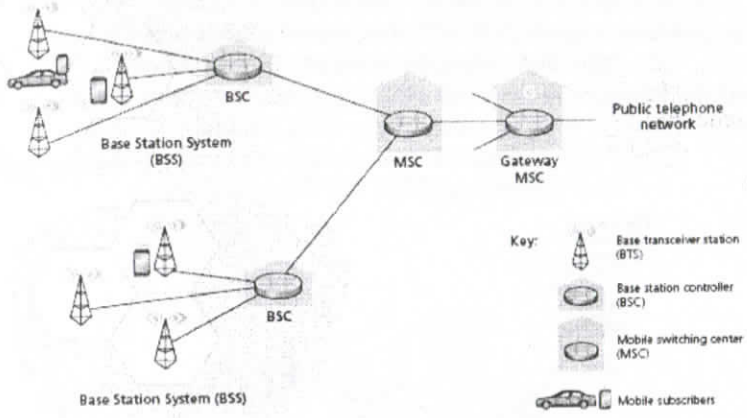



Рис.2.16. Компоненты сети сотовой связи 2G стандарта GSM

Контроллер базовой станции (base station controller BSC) управляет несколькими передающими станциями распределяет выделенные базовой станции BTS радиоканалы между мобильными абонентами.

MSC (mobile switching center) отвечает за соединение базовых станций между собой, организацию связи с другими видами сетей (например, стационарными телефонными сетями) и сотовыми сетями других операторов. При соединении мобильных абонентов разных операторов MSC одного оператора подключается к MSC другого оператора.

Создаётся впечатление, что абоненты сотовой сети подключаются к различным телефонным сетям только для получения телефонных услуг (так называемых голосовых услуг), однако это неверно. Сотовые абоненты могут получать и читать сообщения электронной почты, подключаться к Web, использовать сервисы, связанные с местоположением пользователя от географических карт (Location map) до меню ресторанов, кафе, расписания сеансов в театрах и кинотеатрах, просматривать потоковое видео (streaming video).

Что бы сделать это наш smartphone должен запустить полный стек протоколов (включая физический, сетевой, транспортный

уровни и уровень приложений) и подключиться к Интернет через сеть передачи данных сотового оператора. В качестве примера сетей 3G рассмотрим стандарт UMTS (Universal Mobile Telecommunications Service) 3G standard, разработанный организацией 3GPP (3rd Generation Partnership project), структура сети показана на рис.2.17.

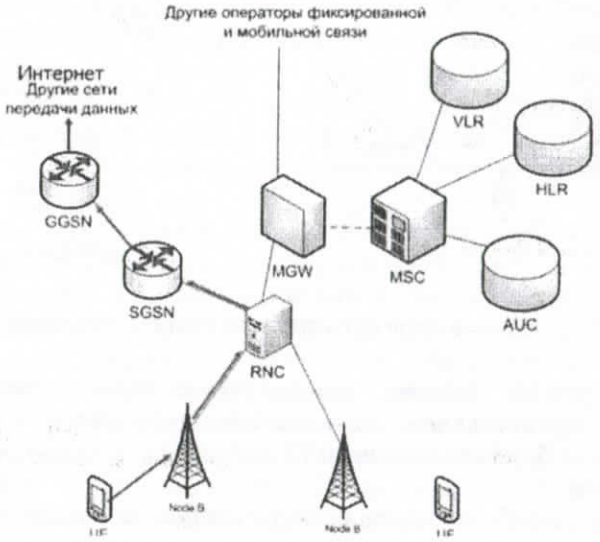



Рис.2.17. Мобильный доступ в Интернет в сети UMTS

Сеть оператора UMTS делится на сеть радиодоступа и опорную сеть Core Network CN. Логически CN в UMTS подразделяется на домен с коммутацией пакетов (PS) и домен с коммутацией каналов (CS). Домен с коммутацией пакетов обеспечивает пакетную передачу данных на основе протоколов TCP/IP, одной из услуг которого является мобильный доступ в Интернет. В состав домена с коммутацией пакетов входят следующие устройства (см.рис.2.17) – сервер MSC (MSC server или MSS), медиашлюз (Media Gateway, MGW), регистр местоположения пользователя (VLR), домашний регистр (HLR), центр аутентификации (AUC) и регистр идентификации оборудования (EIR).

Домен с коммутацией каналов включён в архитектуру для поддержки услуг с коммутацией каналов и совместимости со старым



оборудованием. Использование в области коммутации каналов отдельного сервера MSC и медиашлюза CS-MGW позволило разделить абонентскую плоскость и плоскость управления и географически оптимизировать абонентскую плоскость.

Core network сотовой сети передачи данных 3G соединяет сети радио доступа с сетью интернет-провайдера. Для этого в сети имеется два вида узлов – Serving GPRS Support Nodes (SGSNs) и Gateway GPRS Support Nodes (GGSNs), как показано на рис.2.18[19].

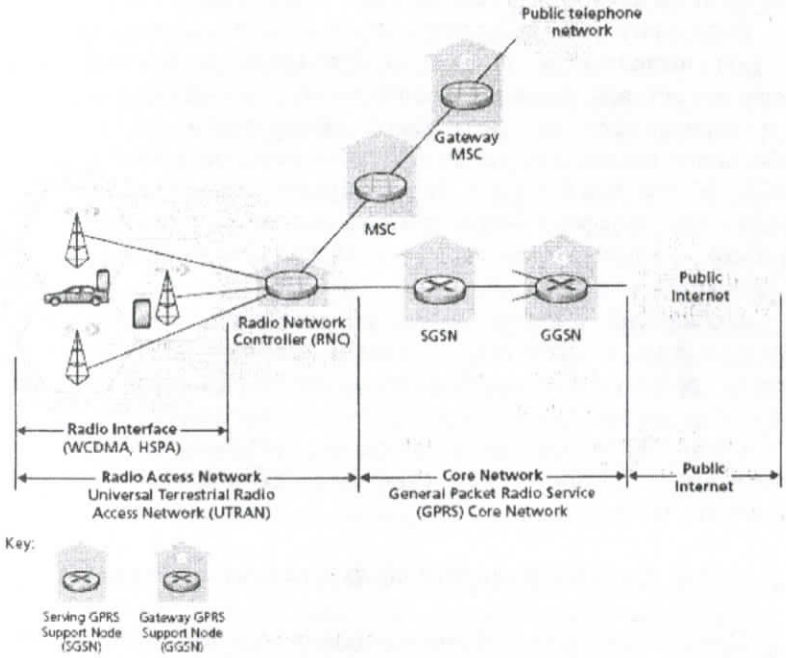



Рис.2.18. Подключение в Интернет через сеть 3G

Узел SGSN отвечает за доставку дейтаграмм к/от узлов мобильной сети к сети радиодоступа, к которой SGSN подключён. SGSN взаимодействует с MSC для авторизации пользователей, предоставления «хэндовера», управления информацией

[19] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

местоположения абонента (в какой соте находится абонент), пересылки дейтаграм между узлами мобильной сети от сети радиодоступа к GGSN и обратно.

GGSN работает как шлюз, соединяющий несколько SGSN с сетью интернет-провайдера. SGSN последний узел инфраструктуры сети 3G, который проходит дейтаграмма на пути от мобильного термина до сети Интернет. Внешний мир сети Интернет рассматривает GGSN как обычный шлюз, GGSN «скрывает» мобильность узлов 3G от остальной структуры Интернет, в которой хост машины являются неподвижными объектами.

Подключение к интернету, через USB-модем или мобильный телефон выполняется за счет «обращения» к базовой станции оператора сотовой связи, у которого вы обслуживаетесь (см.рис.1.35), и в зависимости от того какое оборудование установлено у мобильного провайдера устанавливается связь по технологии GPRS, EDGE, 3G или HSDPA (4G). Таким образом, после соединения USB-модема или телефона (через USB-кабель, инфракрасный порт или Blurtooth) с компьютером вы получите доступ к интернету по одной из упомянутых технологий.

Мобильный интернет имеет не устойчивое качество связи и довольно низкую скорость, но вполне пригодную для нормальной загрузи страниц в браузер. Максимальная скорость передачи данных в представленных технологиях в среднем составляет 20-40кбит/с в GPRS, 100-236кбит/с в EDGE; 144кбит/с - 3,6Мбит/с в 3G и 4G может превышать 100 Мбит/с, а у стационарных абонентов она может составлять 1Гбит/с.

## 2.8. Доступ в Интернет через спутниковые каналы

Для подключения одностороннего спутникового интернета понадобиться небольшой комплект оборудования – спутниковая антенна, усилитель-конвертер (подбирается под диапазон C, Ka или Ku и линейную или круговую поляризацию оператора), спутниковый приемник (PCI-плата или USB-приемник), кабель нужной длины типа RG-6 (75 Ом) и несколько F-разъемов.

Для двустороннего доступа к спутниковому интернету нужна приемопередающая антенна (диаметром около 1,2-1,8м), передающий BUC (block-up converter) и приемный LNB (low-noise block) блок и спутниковый модем, к которому можно подключить не один, а



несколько компьютеров и обеспечить им доступ в Интернет. Использовать диапазон, рекомендованный спутниковым оператором.

У каждого из этих спутниковых подключений к интернету есть свои особенности. Для одностороннего доступа нужен уже существующий доступ в интернет (например, GPRS или EDGE), по которому отправленные запросы поступят в обработку к интернет-провайдеру (одностороннего доступа), а после обработки полученные данные отправят своему клиенту по спутниковому коридору.

При двустороннем доступе в интернет не нужны дополнительные каналы, так как отправка и прием данных осуществляется через спутник. Многие операторы спутникового интернета могут предложить как безлимитные пакеты, так и тариф с оплатой за трафик. Двусторонний спутниковый интернет у некоторых операторов работает быстрее, чем в технологии 3G, а скорость в Ka-диапазоне может составлять 20 Мбит/с.

Недостатком данной технологии можно считать высокую стоимость оснащения, сложность настройки оборудования для технически неподкованного пользователя и большое время отклика (задержка). Обычно используют спутниковый интернет в отдаленных уголках страны, где нет другой приемлемой альтернативы. Использование Wi-Fi маршрутизатора при спутниковом подключении к провайдеру, так же как и в других технологиях, даст возможность раздавать интернет по беспроводной связи и LAN кабелю другим цифровым устройствам (ноутбук, планшет) в доме.

## 2.9. Телекоммуникационные линии связи

Линия связи ЛС – физическая среда, по которой передаются сигналы. Физическая среда передачи данных может представлять собой кабель, т.е. набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны. В зависимости от среды передачи данных различают следующие линии связи:

- проводные (воздушные);
- кабельные (медные и волоконно-оптические);
- радиоканалы наземной и спутниковой связи;
- инфракрасные лучи.

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

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

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Существует много типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью связи.

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

### 2.9.1. Кабельные линии

Кабельные линии состоят из проводников, заключенных в



несколько слоев изоляции: электрической, электромагнитной, механической. На рис.2.19 приведена классификация кабелей.


Рис.2.19. Классификация кабелей

**Витáя пáра** – вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой (см.рис.2.20). В настоящее время, благодаря своей дешевизне и лёгкости в установке, витая пара является самым распространённым решением для построения локальных сетей. Витая пара может быть выполнена в экранированном варианте, когда пару медных проводов обертывает изоляционный экран, и неэкранированном, когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

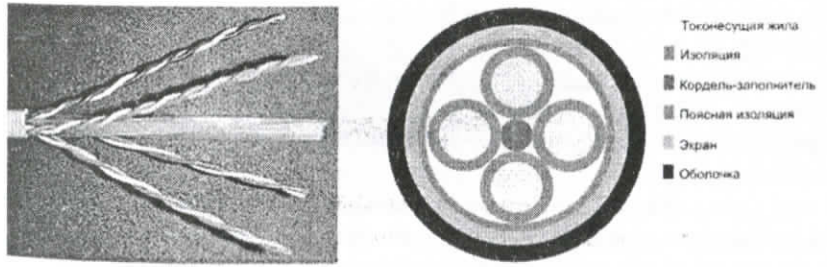



Рис.2.20. Витая пара

**Кабели на основе неэкранированной витой пары** (Unshielded Twisted Pair – UTP) имеют пять категорий с различными характеристиками:

- 1 – телефонный кабель для передачи аналоговых сигналов;
- 2 – кабель из четырех витых пар, скорость 4 Мбит/с;
- 3 – то же, со скоростью 10 Мбит/с;
- 4 – то же, 16 Мбит/с;
- 5 – то же, 100 Мбит/с.

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

**Кабели на основе экранированной витой пары** (Shielded Twisted Pair — STP) хорошо защищают передаваемые сигналы от внешних помех, а также меньше излучают электромагнитных колебаний , что в свою очередь защищает пользователей сетей от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель и усложняет его прокладку, так как требует выполнения качественного заземления. Экранированный кабель применяется только для передачи данных, голос по нему не передают.

**Кабель коаксиальный** — кабель, в котором внутренний провод для снижения радиопомех окружен вторым экранирующим проводом. Имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции (см.рис.2.21).

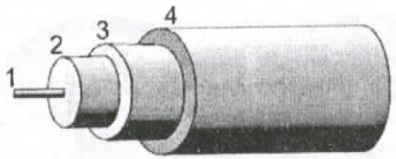



Рис.2.21. Структура коаксиального кабеля
1 – центральный проводник; 2 – изолятор; 3 – проводник-экран; внешний изолятор

Тонкий коаксиальный кабель – гибкий кабель диаметром примерно 0,5см. Он способен передавать сигнал на расстояние до 185



м без его заметного искажения, вызванного затуханием. Волновое сопротивление 50Ом. Толстый коаксиальный кабель — относительно, жесткий кабель диаметром около 1см. Медная жила у этого кабеля толще, чем у тонкого, и, следовательно, сопротивление меньше. Поэтому толстый коаксиальный кабель передает сигналы дальше, чем тонкий, на расстояние до 500м.

### 2.9.2. Волоконно-оптический кабель ВОЛС

Оптоволокно – это стеклянная или пластиковая нить, используемая для переноса света внутри себя посредством полного внутреннего отражения. Оптоволокно может быть использовано как средство для дальней связи и построения компьютерной сети. Оптоволокно состоит из тонких (5...60 мкм) волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля. Он обеспечивает передачу данных с очень высокой скоростью (до 10Гбит/с и выше), лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

ВОЛС предназначены для передачи больших объемов данных на высоких скоростях. Волоконно-оптический кабель состоит из центрального стеклянного или пластикового проводника, окруженного другим слоем стеклянного или пластикового покрытия, и внешней защитной оболочки (см.рис.2.22). Данные передаются по кабелю с помощью лазерного (laser transmitter) или светодиодного передатчика (LED – Light Emitting Diode transmitter), который посылает одно направленные световые импульсы через центральное стеклянное волокно.

Стеклянное покрытие помогает поддерживать фокусировку света во внутреннем проводнике. Сигнал принимается на другом конце фотодиодным приемником (photodiode receiver), преобразующим световые импульсы в электрический сигнал. Существует два основных типа оптических волокон: многомодовое и одномодовое. Диаметр сердцевины у многомодовых волокон в десятки раз превышает длину волны передаваемого излучения, из-за чего по волокну распространяется несколько типов волн (мод). Стандартные диаметры сердцевины многомодовых волокон — 50 и 62мкм. У одномодового волокна диаметр сердцевины обычно равен 5 ... 10мкм.

Скорость передачи данных для волоконно-оптических сетей находится в диапазоне от 100Мбит/с до 2Гбит/с, а данные могут быть

надежно переданы на расстояние до 2км без повторителя. Волоконно-оптический кабель может поддерживать передачу видео и голосовой информации, передачу данных.

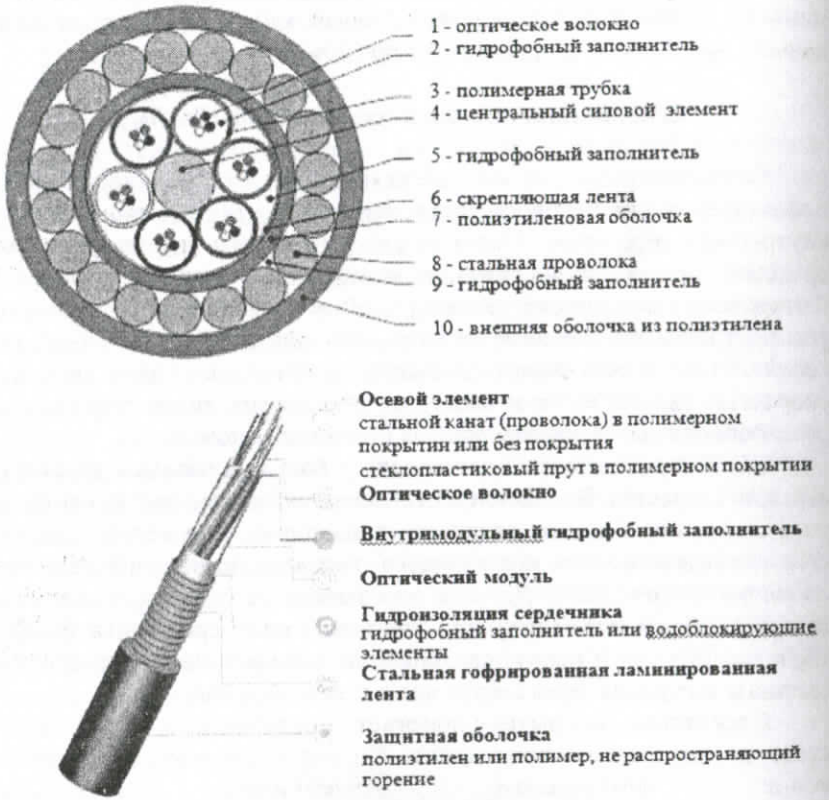



Рис.2.22. Конструкция волоконно-оптического кабеля

Поскольку световые импульсы полностью закрыты в пределах внешней оболочки, волоконно-оптический носитель фактически невосприимчив к внешней интерференции и подслушиванию. Поскольку световые импульсы могут двигаться только в одном направлении, системы на базе волоконно-оптических кабелей должны иметь входящий и исходящий кабели для каждого сегмента, который будет посылать и получать данные.



Волоконно-оптический кабель обладает большой жесткостью и сложен в установке, что делает его самым дорогим типом сетевого носителя. Он требует специальных соединителей — конвекторов и высококвалифицированной установки. Эти факторы приводят к высокой стоимости внедрения. Одним из способов снижения расходов является использование волоконно-оптического кабеля только в сетевых магистралях или в тех линиях, для которых имеют значение влияние электромагнитного наложения, возгораемость и т.п.

### 2.9.3. Радиоканалы

Связь по радиоканалу используется для построения магистралей (радиорелейные линии), для создания локальных сетей, и для подключения удаленных абонентов к сетям и магистралям разного типа (см.рис.2.23). Существуют несколько типов радиоканалов и, соответственно, несколько типов связи – радиосвязь, связь в микроволновом диапазоне, инфракрасная связь. Беспроводная сеть работает там, где не работает кабельная.

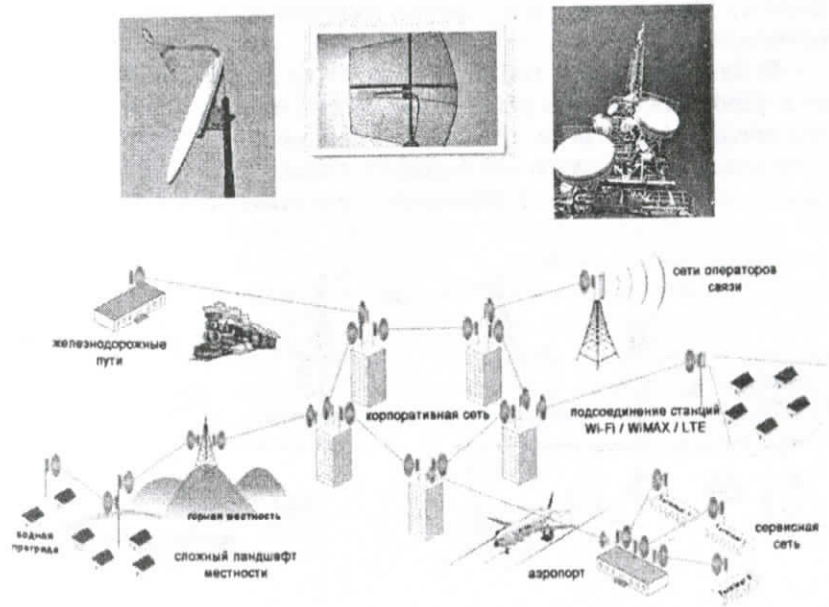



Рис.2.23. Связь по радиоканалу

**Радиосвязь** - пересылка данных осуществляется на радиочастотах, не имеет ограничений по дальности, используется для соединения локальных сетей на больших расстояниях.

Этот вид связи имеет высокую стоимость, подлежит государственному регулированию, крайне чувствительна к электронному и атмосферному наложениям, подвержена перехвату, требует шифрования при передаче, чтобы обеспечить разумный уровень безопасности.

**Радиоканалы наземной и спутниковой связи** образуются с помощью передатчика и приемника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн (КВ, СВ и ДВ), называемые также диапазонами амплитудной модуляции (АМ – Amplitude Modulation) по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы в диапазоне ультракоротких волн (УКВ) с частотной модуляцией (FM – Frequency Modulation) и в диапазоне сверхвысоких частот (СВЧ, или microwaves).

В диапазоне СВЧ (свыше 4ГГц) сигналы уже не отражаются ионосферой Земли, и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы, обеспечивающие выполнение этого условия (см.рис.2.24).

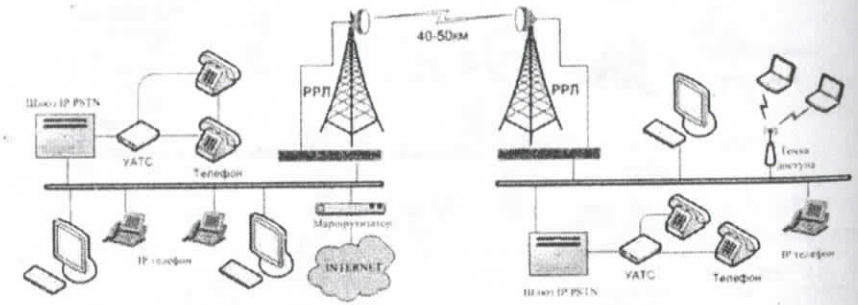



Рис.2.24. Схема радио-релейной связи



Все системы радиосвязи передают информацию посредством, электромагнитных волн радиодиапазона. Однако радиодиапазон занимает только часть спектра электромагнитных волн. Более высокие частоты (непосредственно перед видимым светом) располагаются в инфракрасной части спектра.

**Связь в инфракрасном диапазоне** имеет широкий диапазон частот. Передача осуществляется узким лучом при полном отсутствии боковых излучений. Передатчиком служит - полупроводниковый излучающий диод. В качестве приемника используется высокочувствительный фотодиод. Передача данных в инфракрасном диапазоне использует высокие частоты и применяется как на коротких расстояниях, так и в глобальных масштабах. Главное ограничение - передатчик и приемник должны быть в зоне прямой видимости. Обычно передача данных в инфракрасном диапазоне применяется для соединения локальных сетей в отдельных зданиях, где использование физического носителя затруднено или непрактично, а также в глобальной передаче с помощью спутников и наземных спутниковых антенн, обеспечивающих выполнение требования прямой видимости (см.рис.2.25).

Спутники в системах связи могут находиться на геостационарных (высота 36тыс.км) или низких орбитах. При геостационарных орбитах заметны задержки прохождения сигналов (туда и обратно около 520мс). Возможно покрытие поверхности всего земного шара с помощью четырех спутников. В низкоорбитальных системах обслуживание конкретного пользователя происходит попеременно разными спутниками (см.рис.2.26). Чем ниже орбита, тем меньше площадь покрытия и, следовательно, требуется или большее число наземных станций, или межспутниковая связь, что утяжеляет спутник. Число спутников также значительно больше (обычно несколько десятков). Например, глобальная спутниковая сеть Iridium, имеющая и российский сегмент, включает 66 низкоорбитальных спутников. Диапазон частот составляет 1610 ... 1626,5МГц.

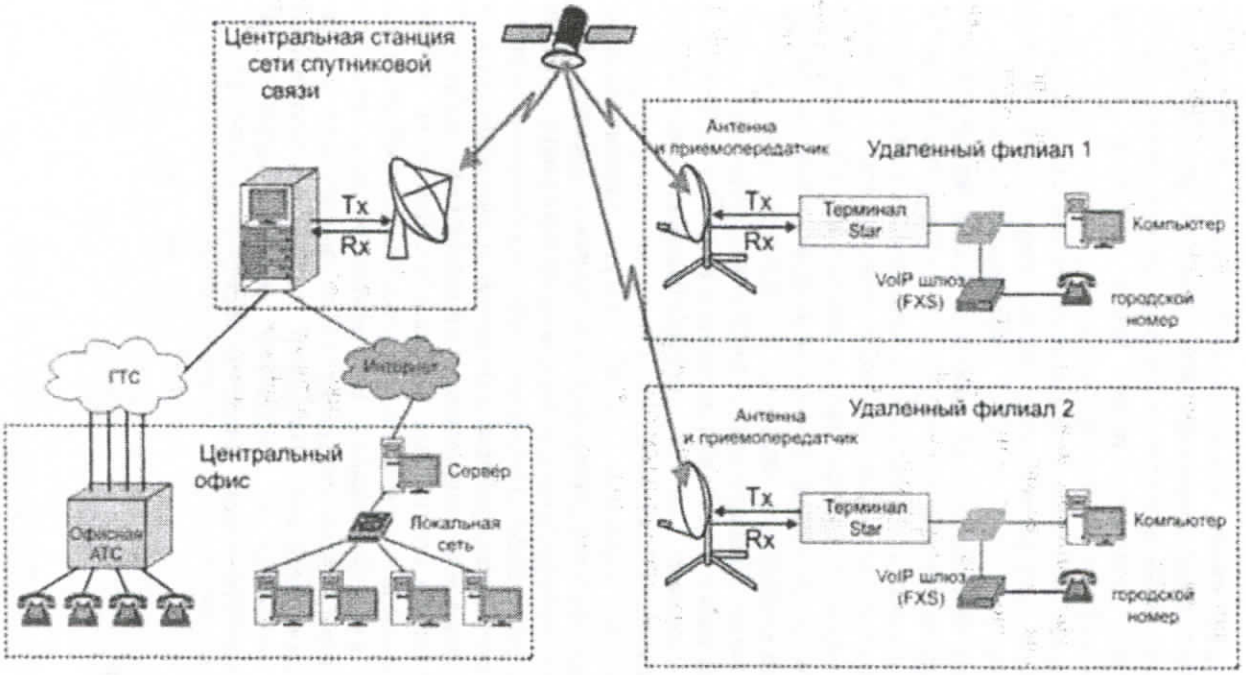



Рис.2.25. Схема спутниковой связи



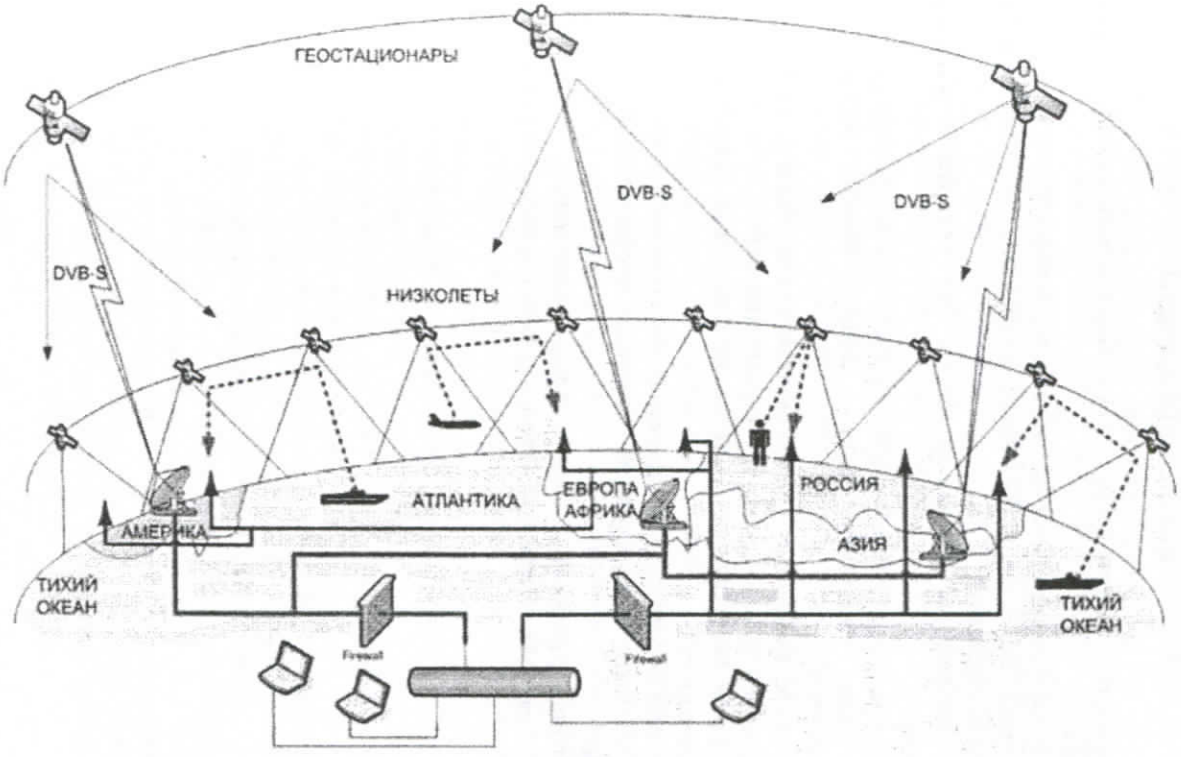



Рис.2.26. Центр управления системой спутниковой связи

## Контрольные вопросы

1. Что входит в понятие доступ к сети? Перечислите способы доступа к Сети.
2. Что такое периферийный маршрутизатор интернет?
3. Что такое Линия связи? Как классифицируются ЛС в зависимости от среды передачи?
4. Как называется физическая среда, по которой передаются сигналы?
5. Что такое проводные (воздушные) линии? Где они применяются?
6. Что такое кабельные медные линии? Какова область их применения?
7. Что такое кабельные волоконно-оптические линии, волоконно-оптический кабель, каковы его характеристики?
8. Что такое беспроводные радиоканалы наземной связи? Где они применяются?
9. Что такое беспроводные радиоканалы спутниковой связи?
10. Что такое беспроводные лазерные, инфракрасные, каналы связи?
11. Что такое витая пара, каковы её характеристики?
12. Что такое коаксиальный кабель, каковы его характеристики?



# 3. ЛОКАЛЬНЫЕ СЕТИ И ИХ КОМПОНЕНТЫ

## 3.1. Локальные сети – общие понятия

Локальная компьютерная сеть – Local Area Network (LAN) – это коммуникационная система, расположенная в пределах одного здания или другой ограниченной территории, поддерживающая один или несколько высокоскоростных цифровых каналов связи, предоставляемых подключённым к ним компьютерам в кратковременное монопольное пользование.

LAN имеет следующие характеристики:

- общая протяжённость 1-2км;
- скорость передачи данных от 1Мбит/с до нескольких Гбит/с;
- простое подключение новых компьютеров и отключение старых без нарушения работы сети;
- равноправный доступ всех рабочих станций к устройствам коллективного доступа (серверам, принтерам);

Исторически главной целью объединения компьютеров в сеть было разделение ресурсов. Пользователи компьютеров, подключенных к сети, или приложения, выполняемые на этих компьютерах, получают возможность автоматического доступа к разнообразным ресурсам остальных компьютеров сети, к числу которых относятся:

- периферийные устройства, такие как диски, принтеры, плоттеры, сканеры и др.;
- данные, хранящиеся в оперативной памяти или на внешних запоминающих устройствах;
- вычислительная мощность (за счет удаленного запуска «своих» программ на «чужих» компьютерах).

Чтобы обеспечить пользователей разных компьютеров возможностью совместного использования ресурсов сети, компьютеры необходимо оснастить некими дополнительными сетевыми средствами.

Для связи устройств в них, прежде всего, должны быть предусмотрены внешние интерфейсы.

**Интерфейс** – в широком смысле – формально определенная логическая и/или физическая граница между взаимодействующими независимыми объектами. Интерфейс задает параметры, процедуры и характеристики взаимодействия объектов[20].

[20] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010

Разделяют физический и логический интерфейсы.

- **Физический интерфейс** (называемый также портом) – определяется набором электрических связей и характеристиками сигналов. Обычно он представляет собой разъем с набором контактов, каждый из которых имеет определенное назначение, например, это может быть группа контактов для передачи данных, контакт синхронизации данных и т.п. Пара разъемов соединяется кабелем, состоящим из набора проводов, каждый из которых соединяет соответствующие контакты. В таких случаях говорят о создании линии, или канала, связи между двумя устройствами.
- **Логический интерфейс** (называемый также **протоколом)** — это набор информационных сообщений определенного формата, которыми обмениваются два устройства или две программы, а также набор правил, определяющих логику обмена этими сообщениями.

*Интерфейс компьютер-компьютер* позволяет двум компьютерам обмениваться информацией. С каждой стороны он реализуется парой:

- аппаратным модулем, называемым сетевым адаптером, или сетевой интерфейсной картой (Network Interface Card, NIC);
- драйвером сетевой интерфейсной карты — специальной программой, управляющей работой сетевой интерфейсной карты.

Сетевой адаптер (Network Interface Card, NIC) – специальная плата, которая устанавливается внутрь системного блока в один из слотов материнской платы. Основная функция - передача и прием информации в сети. На рис.3.1 приведён пример функций сетевого адаптера при доступе в Интернет, связь сетевого адаптера с другими компонентами хоста и функциональностью стека протоколов TCP/IP[21].

*Интерфейс компьютер-периферийное устройство* (например, интерфейс компьютер-принтер) позволяет компьютеру управлять работой периферийного устройства. Этот интерфейс реализуется:

- со стороны компьютера – интерфейсной картой и драйвером периферийного устройства (принтера), подобным сетевой интерфейсной карте и ее драйверу;

[21] J.Kurose, K.Ross. Computer networking A Top-Down Approach. Sixth edition. Pearson Education, 2013



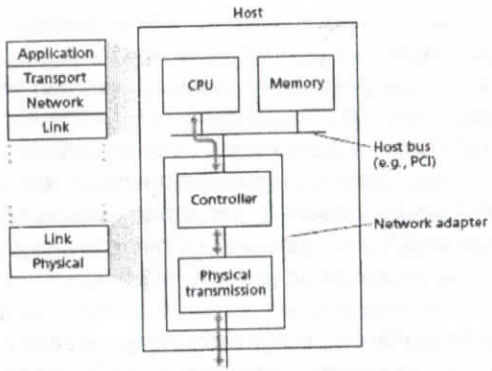



Рис.3.1. Функции сетевого адаптера при доступе в Интернет

- со стороны периферийного устройства – контроллером периферийного устройства (принтера), обычно представляющий собой аппаратное устройство, принимающее от компьютера как *данные,* например, байты информации, которую нужно распечатать на бумаге, так и *команды,* которые он отрабатывает, управляя электромеханическими частями периферийного устройства, например, выталкивая лист бумаги из принтера или перемещая магнитную головку диска.

## 3.2. Сетевое программное обеспечение

Рассматривая связь компьютера с периферийным устройством, мы столкнулись с важнейшими «сетевыми» понятиями: интерфейсом и протоколом, драйвером и интерфейсной картой, а также с проблемами, характерными для компьютерных сетей: согласованием интерфейсов, синхронизацией асинхронных процессов, обеспечением достоверности передачи данных.

Эти функции выполняет **сетевое программное обеспечение**, которое состоит из сетевых служб, сетевой операционной системы и сетевых приложений.

Потребность в доступе к удаленному принтеру может возникать у пользователей самых разных приложений: текстового редактора, графического редактора, системы управления базой данных (СУБД). Очевидно, что дублирование в каждом из приложений общих для всех них функций по организации удаленной печати является

избыточным. Более эффективным представляется подход, при котором эти функции исключаются из приложений и оформляются в виде пары специализированных программных модулей – *клиента* и *сервера печати.* Эта пара клиент-сервер может быть использована любым приложением, выполняемым на компьютере[22].

**Клиент** – это модуль, предназначенный для формирования и передачи сообщений-запросов к ресурсам удаленного компьютера от разных приложений с последующим приемом результатов из сети и передачей Их соответствующим приложениям.

**Сервер** – это модуль, который постоянно ожидает прихода из сети запросов от клиентов, и приняв запрос, пытается его обслужить, как правило, с участием локальной ОС; один сервер может обслуживать запросы сразу нескольких клиентов (поочередно или одновременно).

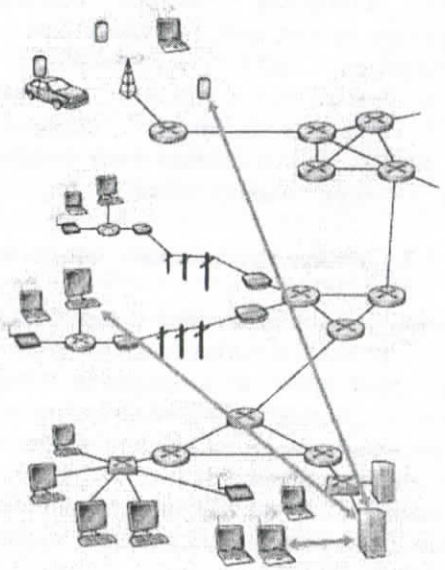


Рис.3.2. Архитектура клиент-сервер на примере веб-службы сети Интернет

[22] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010



На рис.3.2 приведена архитектура клиент-сервер на примере веб-службы сети Интернет[23].Пара клиент-сервер, предоставляющая доступ к конкретному типу ресурса компьютера через сеть, образует **сетевую службу.** Каждая служба связана с определенным типом сетевых ресурсов. Например, модули клиента и сервера, реализующие удаленный доступ к принтеру, образуют сетевую службу печати. Файловая служба позволяет получать доступ к файлам, хранящимся на диске других компьютеров. Серверный компонент файловой службы называют файл-сервером. Для поиска и просмотра информации в Интернете используется веб-служба, состоящая из веб-сервера и клиентской программы, называемой веб-браузером (web browser). Разделяемым ресурсом в данном случае является веб-сайт – определенным образом организованный набор файлов, содержащих связанную в смысловом отношении информацию и хранящихся на внешнем накопителе веб-сервера

### 3.3. Сетевая операционная система

*Операционную систему компьютера* часто определяют как взаимосвязанный набор системных программ, который обеспечивает эффективное управление ресурсами компьютера (памятью, процессором, внешними устройствами, файлами и др.), а также предоставляет пользователю удобный интерфейс для работы с аппаратурой компьютера и разработки Приложений. Говоря о *сетевой операционной системе* (сетевой ОС), мы должны расширить границы управляемых ресурсов за пределы одного компьютера.

**Сетевой операционной системой** называют операционную систему компьютера, которая помимо управления локальными ресурсами предоставляет пользователям и приложениям возможность эффективного и удобного доступа к информационным и аппаратным ресурсам других компьютеров сети. Сегодня практически все операционные системы являются сетевыми[24].

Удаленный доступ к сетевым ресурсам обеспечивается:

- сетевыми службами;
- средствами транспортировки сообщений по сети (в простейшем

[23] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

[24] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010

случае — сетевыми интерфейсными картами и их драйверами).

Сетевая служба может быть представлена в ОС либо обеими (клиентской и серверной) частями, либо только одной из них. В первом случае операционная система, называемая **одноранговой,** не только позволяет обращаться к ресурсам других компьютеров, но и предоставляет собственные ресурсы в распоряжение пользователей других компьютеров. Например, если на всех компьютерах сети установлены и клиенты, и серверы файловой службы, то все пользователи сети могут совместно применять файлы друг друга. Компьютеры, совмещающие функции клиента и сервера, называют одноранговыми узлами.

Операционная система, которая преимущественно содержит клиентские части сетевых служб, называется **клиентской.** Клиентские ОС устанавливаются на компьютеры, обращающиеся с запросами к ресурсам других компьютеров сети. За такими компьютерами, также называемыми **рабочими станциями**, работают рядовые пользователи. Обычно рабочие станции относятся к классу относительно простых устройств.

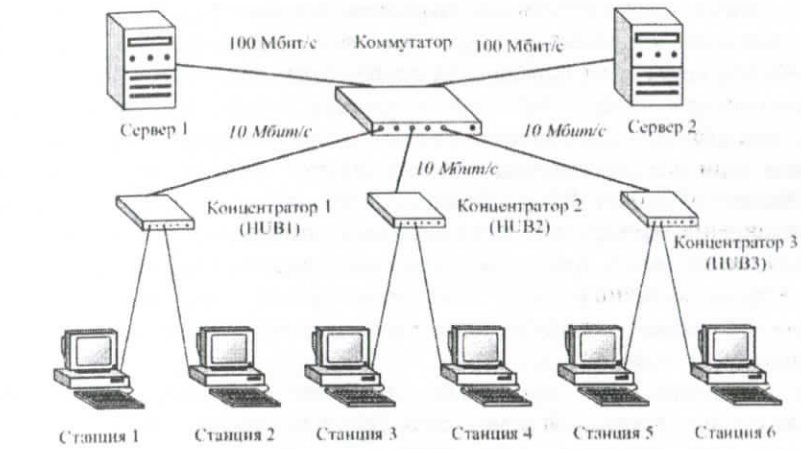
К другому типу операционных систем относится **серверная ОС** — она ориентирована на обработку запросов из сети к ресурсам своего компьютера и включает в себя в основном серверные части сетевых служб. Компьютер с установленной на нем серверной ОС, занимающийся исключительно обслуживанием запросов других компьютеров, называют **выделенным сервером** сети. За выделенным сервером, как правило, обычные пользователи не работают.

### 3.4. Типовой состав оборудования локальной сети

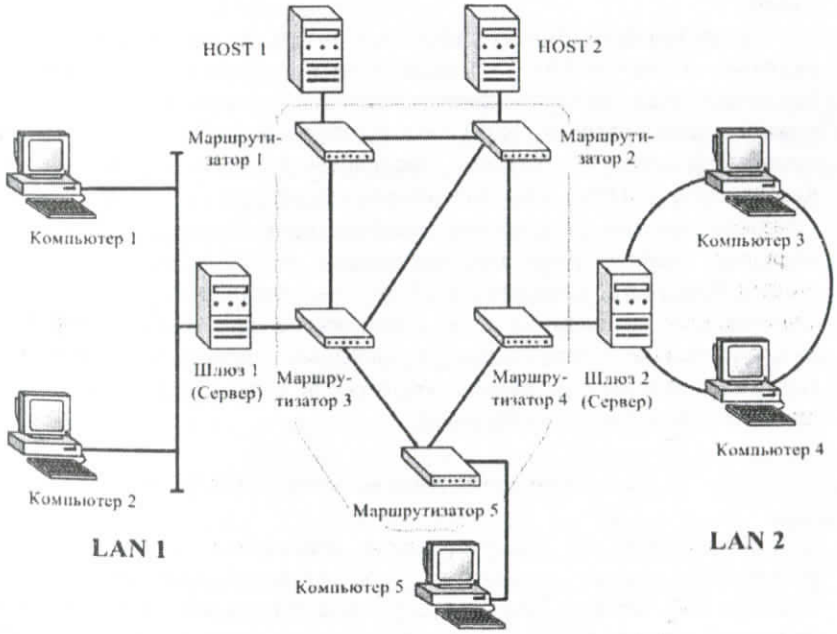
На рис.3.3,а приведена структура коммуникационной подсети, в состав которой входят узлы коммутации (маршрутизаторы) и соединяющие их каналы связи. Сетевыми абонентами могут являться LAN, мощные многопроцессорные компьютеры (host), сетевые терминалы на базе персональных компьютеров[25]. Подключение абонентов к коммуникационной подсети производится с помощью шлюзов, выполняющих преобразование данных и сетевых протоколов.

[25] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.






а)




б)

Рис.3.3. Структура коммуникационной подсети и LAN Ethernet

Мост – это устройство, соединяющее две сети, построенные по одинаковой технологии, например, сети локальные сети Ethernet и ARCnet, через него передаются сообщения, которыми обмениваются компьютеры, расположенные в разных сетях. Маршрутизатор – устройство для соединения отдаленных участков одной локальной сети или для соединения LAN с разной технологией, например, Ethernet и Token Ring. Основное назначение маршрутизатора – управление маршрутами передаваемых сообщений, маршрутизатор в отличие от моста имеет собственный сетевой адрес и используется как промежуточный пункт назначения. Шлюз – устройство, которое кроме функций маршрутизации выполняет преобразование данных из одного формата.

На рис.3.3,б приведена наиболее популярная структура построения локальной сети – сеть Ethernet с топологии звезда, часто такие сети называют сеть Ethernet на основе устройств Hub или Switch[26].

В состав сети входят рабочие станции, за которыми работают рядовые пользователи и выделенные сервера, занимающиеся исключительно обслуживанием запросов других компьютеров, а также концентраторы (Hub) коммутатор (Switch). Все устройства соединены между собой посредством кабеля витая пара. Концентратор (Hub) – интеллектуальное устройство, отвечающее за контроль ошибок, разрешение конфликтов в случае одновременной передачи данных рабочими станциями, имеет стандартное число портов 8,16,24,48. Коммутатор (Switch) – устройство, конструктивно выполненное в виде Hub и работающее как высокоскоростной многопортовый мост, имеет встроенный механизм коммутации, который позволяет разрешать конфликты путем выделения полосы пропускания конечным станциям.

### 3.5. Уровневая модель локальной сети

Комитетом по стандартизации локальных сетей IEEE был разработан проект стандарта LAN, который получил название стандарт 802. Модель LAN стандарта 802 основывается на концепции открытых систем OSI и содержит основные рекомендации, которым

[26] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.



следует руководствоваться при построении конкретных локальных сетей. Модель OSI будет подробно рассматриваться в разделе 5.3, пока приведём некоторые факты, необходимые для понимания модели локальных сетей IEEE 802.

На основании концепции открытых систем Международный институт стандартов (ISO) разработал семиуровневую модель компьютерной сети , которая получила название «модель ISO/OSI». В соответствии с моделью взаимодействие пользователей через коммуникационную подсеть производится с помощью сетевых протоколов.

Под сетевым протоколом понимается строго формализованная процедура (определённая последовательность правил) взаимодействия пользователей сети через коммуникационную подсеть. Между уровнями модели и сетевыми протоколами имеет место определённое соответствие. В таблице 3.1 приведены функции протоколов каждого уровня[27].

Основные отличия модели OSI и модели IEEE 802 – LAN приведены на рис.3.4.

Как рассматривалось в разделе 3.1, каждый компьютер, подключенный к локальной сети, должен иметь специальную плату (сетевой адаптер). Между собой компьютеры (сетевые адаптеры) соединяются с помощью кабелей или радиоканалом, которые называются физической средой передачи данных LAN.

Физическая среда – самый нижний уровень сети. В качестве физической среды передачи данных в LAN может использоваться коаксиальный кабель, витая пара, ВОЛС, инфракрасные и радиоканалы. Характеристики среды передачи влияют на длину сети (на каком расстоянии компьютеры могут располагаться друг от друга) и на скорость передачи данных в локальной сети (см. табл.3.2). Отметим ещё раз, сетевой адаптер – специальная плата, которая устанавливается внутрь системного блока в один из слотов материнской платы. Основная функция – передача и прием информации в сети. Тип устройства, с помощью которого компьютер подключается к физической среде, определяется линией связи ЛС, топологией LAN и принципом передачи сигналов.

[27] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.

Таблица 3.1.

Функции протоколов уровней

| Наименование уровня | Наименование протокола | Функции протокола |
|---|---|---|
| 7.Прикладной уровень | Протокол прикладного уровня | Управление вычислительными процессами, доступом к внешним устройствам, административное управление сетью |
| 6.Представительный уровень | Протокол представительного уровня | Доступ к файлам данных и командным файлам (локальным), преобразование данных в требуемый формат, подготовка эмуляторов программ к работе |
| 5.Сеансовый уровень | Протокол сеансового уровня | Формирование каталога сетевых процессов, установление логического соединения с удаленными процессами, завершение сеанса связи |
| 4.Транспортный уровень | Протокол транспортного уровня | Передача файлов данных и доступ к удаленным файлам, передача и удалённое управление командными файлами, фрагментация и сборка передаваемых сообщений |
| 3.Сетевой уровень | Протокол сетевого уровня | Установление и закрытие логических соединений через коммуникационную подсеть, управление потоками данных и маршрутами движения сообщений (пакетов) |
| 2.Канальный уровень | Протокол канального уровня | Управление передачей и приёмом сообщений (кадров), контроль ошибок, формирование сообщений (кадров) |
| 1.Физический уровень | Протокол физического уровня | Установление и разъединение физических соединений, управление сигнализацией и тактированием |



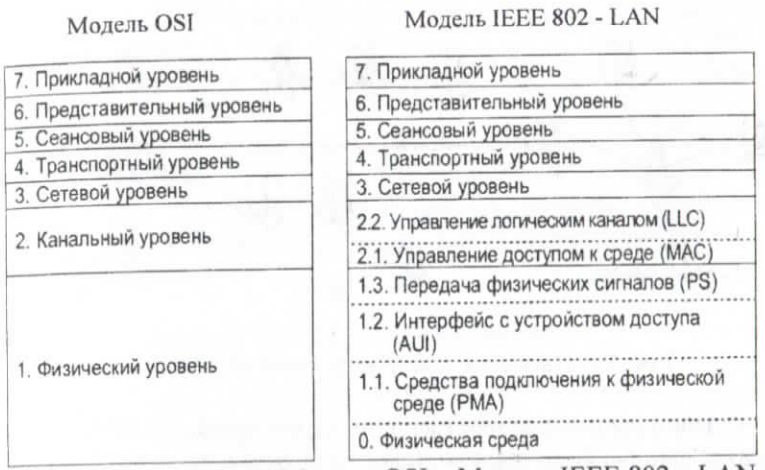



Рис.3.4. Основные отличия Модели OSI и Модели IEEE 802 – LAN

Таблица 3.2

Зависимость длины сети и на скорости передачи данных в локальной сети от среды передачи

| Компьютерный канал связи | Расстояние | Скорость |
|---|---|---|
| Неэкранированная витая пара | До 90 м | 10 – 155 Мбит/с |
| Экранированная витая пара | До 300 м | 16 Мбит/с |
| Коаксиальный кабель | До 2 км | 2 – 44 Мбит/с |
| Оптоволоконный кабель | До 10 км | До 10 Гбит/с |

Топология – это способ соединения компьютеров в сети. Наиболее распространенными способами являются – шина, звезда, кольцо (см.рис.3.5).

Управление доступом к среде зависит от способа передачи данных и делится на различные типы:

- множественный доступ (доступ к каналу связи в режиме соперничества)
- доступ с передачей маркера (пакет, дающий право на передачу данных)
- сети с опросом
- сети с сегментированной передачей
- сети с резервированием времени передачи

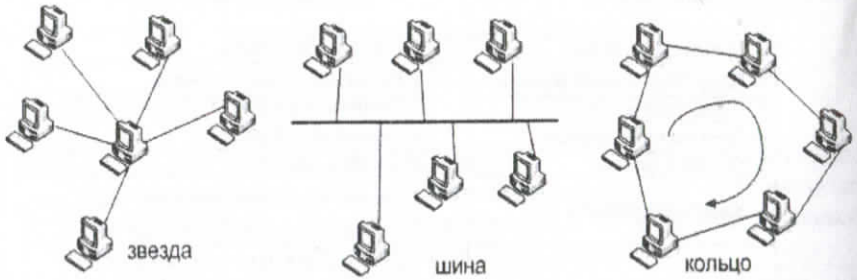



Рис.3.5. Наиболее распространенные топологии LAN

Наибольшее распространение получили LAN топологий шина, звезда и кольцо с множественным доступом и передачей маркёра.

Канальный уровень делится на 2 подуровня (см.рис.3.6):

- управление логическим каналом LLC (Logical Link Control) – не зависит от топологии сети и метода доступа – стандарт 802.2,
- управление доступом к среде MAC.

| Управление логическим каналом | Подуровень LLC IEEE 802.2 | Подуровень LLC IEEE 802.2 | Подуровень LLC IEEE 802.2 |
|---|---|---|---|
| Управление доступом к среде | Подуровень MAC IEEE 802.3 Множественный доступ с контролем несущей и обнаружением столкновений (CSMA/CD) | Подуровень MAC IEEE 802.4 Передача маркера | Подуровень MAC IEEE 802.5 Передача маркера |
| Физический уровень | Шина, звезда | Шина, звезда | Кольцо |

Рис.3.6. Структура канального уровня LAN

Подуровень MAC определяет топологию сети и метод доступа к каналу передачи данных. На этом подуровне определены 3 основных стандарта LAN:

- IEEE 802.3 – LAN топологии шина или звезда с множественным доступом, контролем несущей и обнаружением коллизий (столкновений) - Ethernet



- IEEE 802.4 – LAN топологии шина или звезда с маркерным доступом - ARCnet
- IEEE 802.5 – LAN топологии кольцо с маркерным доступом – Token Ring

Верхние уровни модели IEEE 802 – сетевой, транспортный, сеансовый, представительный и прикладной – не зависят от топологии сети и метода доступа к каналу передачи данных, их программное обеспечение ПО универсально и может применяться в LAN различных типов.

### 3.5.1. IEEE 802.3 – LAN Ethernet

Локальная сеть стандарта IEEE 802.3 – LAN Ethernet разработана компаниями Xerox, DEC, Intel. В качестве среды передачи может использоваться коаксиальный кабель (500м – 1 участок, 1500м макс), витая пара (185м), ВОЛС.

Для построения LAN Ethernet топологии шина используется коаксиальный кабель и устройства повторители и приёмо-передатчики (см.рис.3.7)[28]. Устройство повторитель LAN Ethernet – опознает несущую (физический сигнал передачи данных) и конфликты в одном участке кабеля и регенерирует состояние сети и поток данных на другом участке. Назначение приёмо-передатчиков – согласование параметров сигнала коаксиального кабеля с параметрами шины сетевого контроллера, обнаружение конфликтов.

Для построения LAN Ethernet топологии звезда (см.рис.7.5) в качестве среды передачи используется витая пара, ВОЛС и два вида устройств – концентраторы и коммутаторы[29]. Концентратор (Hub) – это интеллектуальное устройство, контроль ошибок, разрешение конфликтов в случае одновременной передачи данных рабочими станциями. Число портов концентратора может быть 8,16,24,48. Коммутатор (Switch) – устройство, конструктивно выполненное в виде Hub и работающее как высокоскоростной многопортовый мост. Имеет встроенный механизм коммутации, который позволяет разрешать конфликты путем выделения полосы пропускания конечным станциям.

---

[28] [29] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.


Рис.3.7. Ethernet – топология шина

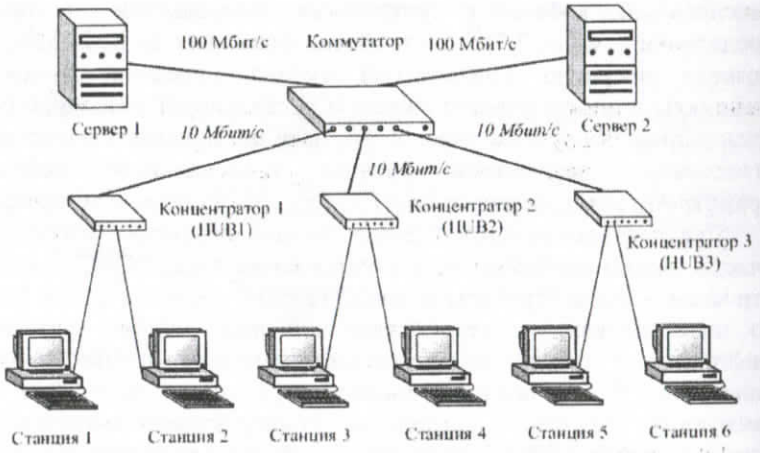



Рис.3.8. Ethernet – топология звезда

В зависимости от среды передачи существуют следующие стандарты Ethernet:

- Thick Ethernet
  - 10Base-T 10Мбит/с 100м UTP
  - 10Base-F 10Мбит/с 2км ВОЛС
- Fast Ethernet - общее название для стандартов передачи данных в сетях по технологии Ethernet со скоростью до 100Мбит/с, в отличие от исходных 10 Мбит/с
  - 100Base-VG 100Мбит/с 100м UTP
  - 100Base-LX10 100Мбит/с 10км ВОЛС
- Gigabit Ethernet – (GbE) Ethernet со скоростью 1 Гбит/с
  - 1000Base-TX 1000Мбит/с 100м UTP
  - 1000Base-LX10 1000Мбит/с 10км ВОЛС
  - 1000Base-EX 1000Мбит/с 40км ВОЛС
  - 1000Base-ZX 1000Мбит/с 70км ВОЛС
- 10 Gigabit Ethernet (10GbE) - 10 Гбит/с
- 100-гигабит Ethernet (100GbE) - скорость передачи данных в 40 и 100 Гбит/с.



### 3.5.2. IEEE 802.4 – LAN ARCnet

Сеть стандарта LAN ARCnet относится к классу сетей с передачей маркера. Маркер – заранее определённая комбинация битов, передаваемая от станции к станции в определённой последовательности. Станция может передавать данные только после поступления к ней маркера и должна передать его дальше в течение короткого интервала времени.

Данный тип сети разработан компанией Datapoint и использует топологию шина или звезда. В качестве среды передачи может использоваться коаксиальный кабель, витая пара. Максимальная длина сети 6,5км. Скорость передачи данных 2,5Мбит/с.

Рассмотрим принцип передачи данных в ARCnet (см.рис.3.9)[30]. Каждый узел идентифицируется собственным адресом MID. Каждому узлу известен идентификатор следующего узла в логическом кольце NID, к которому надо передать маркер. Обычно, следующая станция имеет больший адрес. Во время нормальной работы каждая станция (кроме передающей) находится в состоянии прослушивания канала. Если заголовок приходящего кадра содержит адрес данной станции, то она переходит в состояние приёма и обрабатывает принятый кадр.

[30] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.

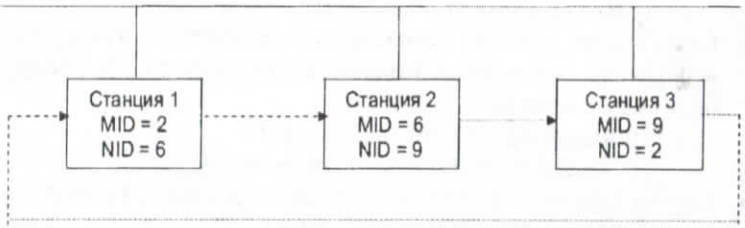



Рис.3.9. Передача данных в ARCnet

Если принятый кадр содержит пакет данных LLC, то он передаётся верхнему уровню, а станция возвращается в состояние прослушивания канала. Если принятый кадр является маркером, то станция получает право передачи кадра. Если имеется пакет данных, поступивший с верхнего уровня, то его передают. После завершения передачи пакета, выполняется передача маркера. При отсутствии пакета передаётся маркер и станция переходит в состояние прослушивания канала.

Сети стандарта ARCnet нашли применение для построения систем управления производственными процессами. В отличии от Ethernet, каждой промышленной установке гарантирован доступ у каналу передачи данных в требуемые интервалы времени, которые необходимы для организации непрерывного технологического процесса.

Перспективами развития сетей стандарта ARCnet являются:

- замена на ВОЛС,
- повышение скорости передачи и протяжённости сети,
- повышение производительности концентраторов и коммутаторов.

### 3.5.3. IEEE 802.5 – LAN Token Ring

Сеть стандарта IEEE 802.5 – LAN Token Ring разработана IBM. Для построения используется коаксиальный кабель, витая пара, ВОЛС. Скорость передачи данных – 4Мбит/с, 16Мбит/с. В качестве структуры сети предлагается однонаправленное физическое кольцо с передачей маркёра, максимальная длина кольца практически неограниченна, максимальное расстояние между соседними станциями 2км. необходимо отметить, что повреждение отдельного узла или кабельного сегмента физического кольца разрушает путь следования сигналов и всю сеть.



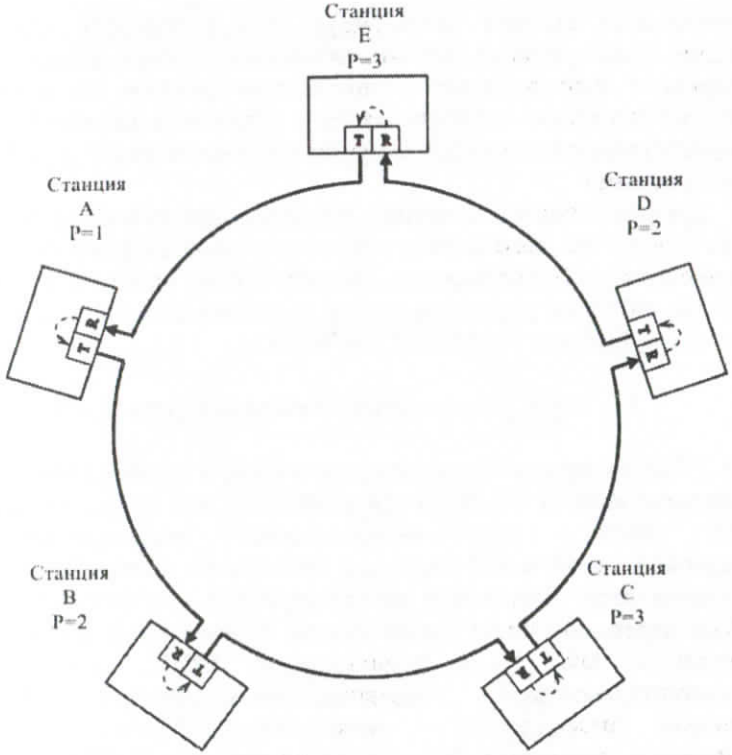



Рис.3.10. Передача данных в Token Ring

На канальном уровне для передачи данных используются кадры типов «маркер» и «информационный кадр». Маркерное кольцо строится на основе приоритетов. Для обеспечения доступа к сети используется маркер. Маркер непрерывно циркулирует по кольцу (см.рис.3.10), проходя через каждую станцию, и содержит индикатор, указывающий свободно или занято кольцо[31]. Если станция желает передать данные и маркер свободен, она захватывает кольцо, превращая маркер в начало информационного кадра, добавляя данные, и посылает кадр по кольцу к следующей станции. Каждая станция анализирует принятый маркер. Если маркер занят,

[31] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.

принимающая станция регенерирует его и передаёт следующей станции. Если принятые данные принадлежат данной станции, то они копируются и отправляются к прикладным уровням. После возврата кадра на исходную станцию, которая произвела передачу, маркер инициализируется (восстанавливается в исходном виде) и передаётся снова в кольцо.

Данный стандарт позволяет строить кольцевую сеть длиной до 50км, однако эти сети характеризуются низкой скоростью передачи данных и низкой надёжностью. Перспективами развития Token Ring является создание двунаправленной высоконадёжной сети FDDI со скоростью передачи 100Мбит/с для WAN.

### 3.6. FDDI – технология глобальной сети WAN

Сеть FDDI базируется на оптическом кабеле и является технологией глобальной сети WAN. Хотя основная среда для передачи данных в FDDI ВОЛС, при использовании экранированной и неэкранированной витой пары эту технологию можно применять в локальной сети. Логическая топология FDDI – кольцо, физическая кольцо деревьев. Общая длина кольца 100км, максимальное число станций – 500. Из-за использования ВОЛС сеть обладает нечувствительностью к электромагнитным помехам и большой степенью безопасности – информацию трудно перехватить удалёнными приборами. Отказоустойчивость сети FDDI (см.рис.3.11) обеспечивается 2 кольцами передачи данных[32]. В нормальном состоянии данные передаются только по основному кольцу. При одиночном физическом разрыве (повреждение отдельного узла или кабельного сегмента) станции по обе стороны разрыва обнаруживают неисправность и автоматически переключают поток данных на резервное кольцо в направлении противоположном направлению передачи по основному кольцу.

Основные типы устройств, используемые FDDI:

- Dual Attachment Concentrator DAC - концентратор с двойным подключением к магистральной сети, участвует в восстановлении кольца;
- Single Attachment Concentrator SAC - концентратор с одиночным

[32] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.



подключением , никогда не подключается к магистральной сети, а только к другому концентратору;

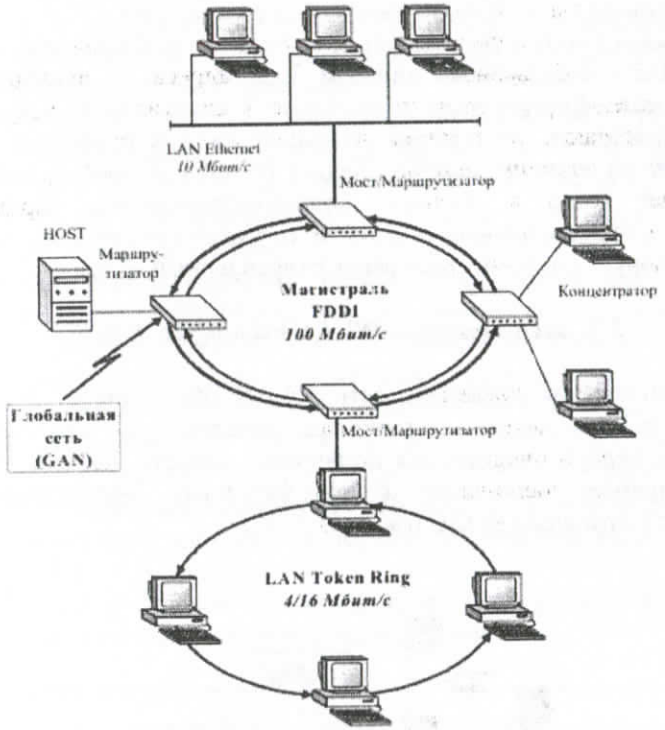



Рис.3.11. Сеть FDDI

- Null Attachment Concentrator NAC – не подключается к магистральному кольцу, а использует FDDI в качестве внутренней магистрали;
- Dual Attachment Station DAS – станция с двойным подключением к магистральному кольцу или концентратору, может участвовать в восстановлении кольца.

Передача данных в FDDI проходит в несколько этапов:

1. Захват маркера станцией -отправителем
2. Передача данных станцией –отправителем

3. Получение кадра другими станциями и возвращение его в кольцо
4. Считывание кадра станцией-получателем и возвращение его в кольцо
5. Удаление кадра из кольца станцией –отправителем

Каждая станция по очереди принимает кадр и сравнивает адрес назначения с собственным адресом. Если адреса не совпадают, то станция регенерирует кадр и посылает к следующему узлу. Если адреса совпадают, то станция помещает кадр в приёмный буфер, проверяет на наличие ошибок, делает отметку о приёме данных и возвращает кадр в кольцо. Станция–отправитель определяет, успешно ли доставлен кадр, и если да, то удаляет его из сети, если нет – регенерирует его (повторяет ранее отправленный кадр).

### 3.7. Беспроводные WLAN стандарта 802.11

Беспроводная локальная сеть WLAN обеспечивает дальность связи на десятки метров от точки беспроводного доступа. Эти сети удобны в первую очередь для подвижных средств. Базовая станция имеет прямое соединение с периферийным маршрутизатором Интернет с помощью ВОЛС (см.рис.3.12)[33].

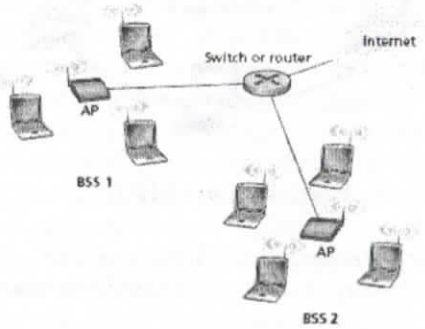



Рис.3.12. Архитектура IEEE 802.11 LAN

Для построения сети WLAN используются устройства Wi-Fi адаптеры и точки доступа. Адаптер – устройство, подключающееся

[33] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



через слот USB, имеет те же функции, что и сетевая карта в проводной сети, служит для подключения компьютера к беспроводной сети. Точка доступа – автономный модуль со встроенным микрокомпьютером и приёмно-передающим устройством, через которое производится взаимодействие и обмен информацией между Wi-Fi адаптерами.

Технология беспроводных сетей развивается довольно быстро. Наиболее перспективным представляется проект IEEE 802.11, который должен играть для радиосетей такую же интегрирующую роль, как 802.3 для сетей Ethernet и 802.5 для Token Ring. Технологии беспроводных сетей семейства 802.11b Wi-Fi (802.11b – Wireless Fidelity) обеспечивают передачу данных в диапазоне 2.4ГГц со скоростью 1, 2, 5,5 и 11Мбит/с. Эта технология WLAN получила массовое распространение в учебных, коммерческих, развлекательных организациях, а также домашнем пользовании.

В протоколе 802.11 используется тот же алгоритм доступа и подавления столкновений, что и в 802.3, но здесь вместо соединительного кабеля используются радиоволны (рис.3.12). Применяемые здесь модемы могут работать и в инфракрасном диапазоне, что бывает привлекательно, если все машины размещены в общем зале.

На рис.3.13 приведены структура канального уровня WLAN и частотный диапазон для построения радиоканалов[34].

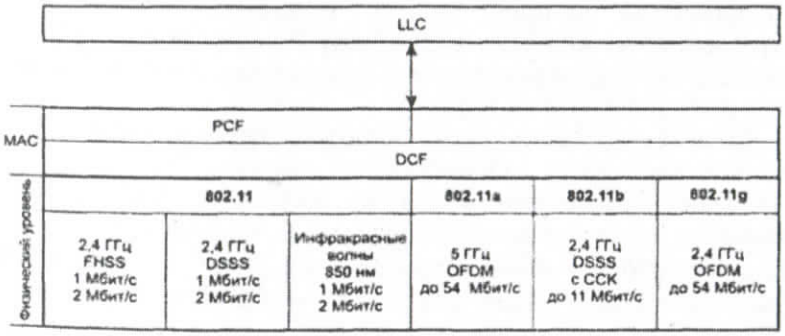



Рис.3.13. Структура канального уровня WLAN

[34] В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.

В отличие от проводной контролируемой среды передачи Ethernet протокол 802.11 MAC доступа к беспроводной среде не выполняет проверку на коллизии и поэтому должен обладать более сильными и масштабируемыми свойствами для минимизации объема необходимой служебной информации управления доступом к среде.

Стандарт 802.11 предполагает работу на частоте 2.4-2.4835ГГц при использовании модуляции 4FSK/2FSK FHSS и DSSS (Direct Sequence Spread Spectrum), мощность передатчика 10мВт-1Вт. В данном частотном диапазоне определено 79 каналов с полосой 1Мбит/с каждый. Максимальная пропускная способность сети составляет 2Мбит/с (в условии малых шумов). Первая локальная сеть 802.11a использовала метод OFDM (Orthogonal Frequency Division Multiplexing). Существует несколько модификаций стандарта и соответствующих регламентирующих документов IEEE 802.11):

802.11D – AdditionalRegulatoryDomains

802.11E – Quality of Service

802.11F – Inter-Access Point Protocol (IAPP)

802.11G — High data rates at 2.4 GHz

802.11H – Dynamic Channel Selection and Transmission Power Control

802.11i – Authentication and Security

Существуют каналы, работающие в инфракрасном диапазоне (850 или 950нм). Здесь возможны две скорости передачи: 1 и 2Мбит/с. При скорости 1Мбит/с используется схема кодирования с группированием четырех бит в 16-битовое кодовое слово, содержащее 15 нулей и одну 1 (код Грея). При передаче со скоростью 2Мбит/с 2 бита преобразуются в 4-битовый код, содержащий лишь одну 1 (0001, 0010, 0100 и 1000)[35].

Следует учитывать, что беспроводные каналы шумны и малонадежны, этому способствуют наводки от СВЧ-печей, работающих практически в том же частотном диапазоне. Если вероятность искажения одного бита равна $p$, вероятность того, что n-битовый кадр будет принят корректно, равна $(1-p)^n$. Для Ethernet кадра максимальной длины при $p=10^{-4}$ вероятность безошибочной доставки составит менее 30%. При $p=10^{-5}$ будет искажаться один из 9 кадров. По этой причине при работе с радиоканалами следует ориентироваться на короткие кадры.

[35] Материалы курса «Высокоскоростные сети связи» http://www.INTUIT.ru



Топологически локальная сеть IEEE 802.11b строится вокруг базовой станции, через которую производится связь с Интернет. Но возможны схемы с несколькими базовыми станциями. Сети 802.11 характеризуются 3 типами топологий:

– независимый набор базовых служб (IBSSs);

– набор базовых служб (BSSs);

– расширенный набор базовых служб (ESSs).

Набор служб (service set) - это логическое группирование сетевых устройств. WLAN предоставляет сетевой доступ посредством широковещательной передачей сигнала на радионесущей, при котором приемная станция принадлежит определенному диапазону передатчиков. Каждый передатчик предваряет процесс передачи сигналом идентификатора сервисного набора (SSID). Приемник использует значение SSID для фильтрации принимаемых сигналов и выделения одного из них.

Сеть независимого набора IBSS состоит из группы устройств 802.11, непосредственно связывающихся друг с другом. Часто такие сети называют ad-hoc сетями, т.к. по существу представляют беспроводные сети «точка – точка». На рис.3.14,а представлены три станции с сетевыми интерфейсами, формирующие IBSS WLAN. Сеть набора IBSS создается, когда отдельные клиентские устройства образуют само формирующуюся сеть без использования точки доступа. Сеть характеризуется малыми размерами и отсутствием распределенных средств хранения информации общего пользования.

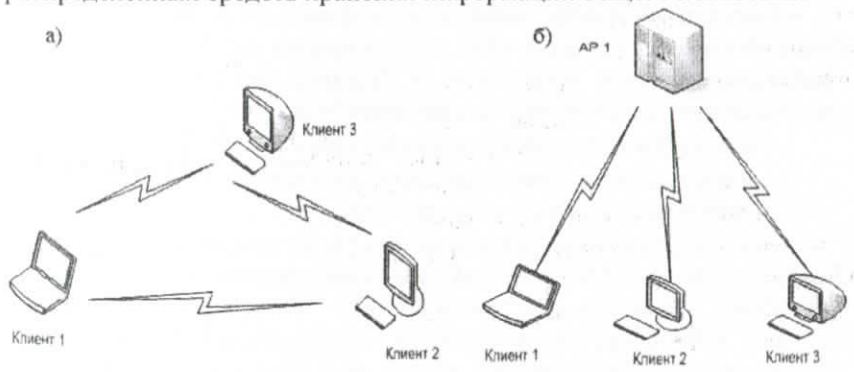



Рис.3.14. Примеры организации WLAN
а) структура IBSS сети б) структура BSS сети

В отличие от сети ESS, две клиентские машины связываются напрямую, создавая базовую сеть BSS без интерфейса к проводным сетям, т.е. в данной сетевой структуре нет систем распределения, связывающих отдельные сети BSS в сеть ESS. Стандартами число сетевых устройств в IBSS не ограничивается. Т.к. сетевые устройства являются устройствами «клиентского» класса, то возможны ситуации, когда устройства не могут взаимодействовать из-за возникновения скрытого шума. При этом отсутствует механизм задержки передачи в IBSS.

Из-за отсутствия точки доступа, тактирование управляется распределенным способом. Новый клиент IBSS устанавливает сигнальный отсчет для создания набора целевых сигнальных интервалов передачи.

Сеть BSS кроме клиентов 802.11 включает в себя специальную клиентскую станцию – точку доступа (access point AP). Точка AP является центральной точкой сети BSS для всех машин сети. Две клиентские машины взаимодействуют друг с другом через точку AP, перенаправляющую информацию между клиентами. Точка доступа может быть оборудована каналом uplink для связи с проводными сетями. Типичная инфраструктура BSS приведена на рис.3.14,б.

Множественная инфраструктура BSS может быть объединена посредством uplink каналов. В сетях 802.11 uplink интерфейс, реализованый как проводной Ethernet канал, соединяет BSS с системой распределения.

Высокие скорости передачи, низкие временные задержки, высокий уровень качества QoS обслуживания являются основными требованиями сетей проводного и беспроводного доступа. Новые предлагаемые услуги опираются на потребности пользователей:

- в доступности широкополосных услуг в любой обстановке;
- в доступности к персональным широкополосным услугам вне зависимости от типа сети доступа;
- в доступности широкополосных услуг по приемлемым ценам.

Локальные сети (LAN) представлены повсеместно как универсальная платформа объединения разнородных устройств, обладающая большой гибкостью по расширению. Беспроводные сети становятся все более распространенными в силу простоты их развертывания и использования.



## Контрольные вопросы

1. Дайте определение локальной сети, назовите её характеристики
2. Как физическая среда влияет на скорость передачи данных в локальной сети?
3. Что такое сетевой адаптер? Чем определяется тип устройства, с помощью которого компьютер подключается к физической среде
4. Что такое топология LAN, виды топологий LAN вы знаете?
5. Какие существуют виды управления доступом к среде LAN? Назовите наиболее распространённые виды управления доступом к среде LAN
6. Какие функции выполняют устройства повторитель LAN Ethernet и приёмо-передатчик Ethernet?
7. Каково назначение концентратора (Hub) и коммутатора (Switch)?
8. Какова скорость передачи в стандарте Ethernet?
9. Что такое маркер, в каких сетях используется?
10. Где применяются сети ARCnet?
11. Где применяется технология FDDI?
12. Какие виды устройств, применяемых в WLAN?
13. В чём отличие протокола доступа к беспроводной среде 802.11 MAC от проводной контролируемой среды передачи Ethernet?
14. Почему необходимо минимизировать объем необходимой служебной информации управления доступом к среде в протоколе 802.11 MAC?
15. Какие типы топологий имеются в сети 802.11?

# 4. КОММУТАЦИЯ И МАРШРУТИЗАЦИЯ В ИНТЕРНЕТ СЕТЯХ

## 4.1. Коммутация определение

Пусть компьютеры физически связаны между собой в соответствии с некоторой топологией и выбрана система адресации (см.рис.4.1). Остаётся нерешённой самая важная проблема – каким способом передавать данные между конечными узлами?[36]

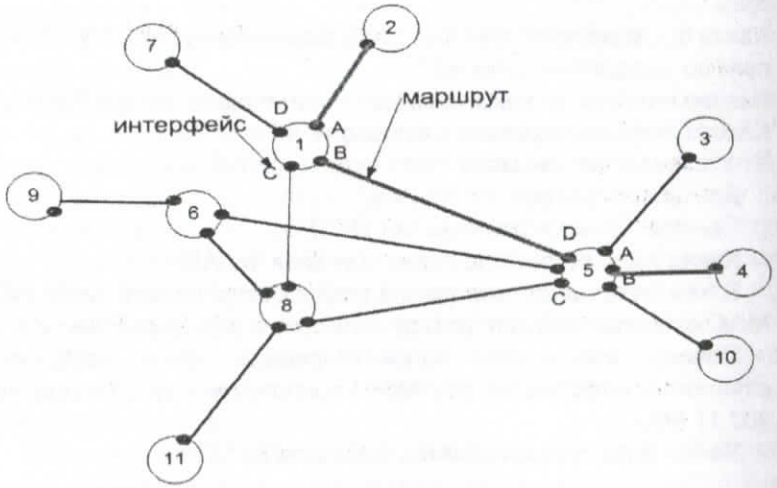



Рис.4.1. Коммутация пользователей через сеть транзитных узлов

Соединение конечных узлов через сеть транзитных узлов называют коммутацией. Последовательность узлов, лежащих на пути от отправителя к получателю, образует маршрут.

Например, в сети, приведённой на рис.4.1, узлы 2 и 4 непосредственно между собой не связаны и вынуждены передавать данные через транзитные узлы, например узлы 1 и 5. Узел 1 должен выполнить передачу данных между своими интерфейсами A и B, а узел 5 – между интерфейсами F и B. В данном случае маршрутом

[36] В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010



является последовательность: 2-1-5-4, где 2 - узел-отправитель, 1 и 5 - транзитные узлы, 4 — узел-получатель.

В общем виде задача коммутации может быть представлена в виде следующих взаимосвязанных частных задач

1. Определение информационных потоков, для которых требуется прокладывать маршруты.
2. Маршрутизация потоков.
3. Продвижение потоков, т.е. распознавание потоков и их локальная коммутация на каждом транзитном узле.
4. Мультиплексирование и демультиплексирование потоков.

Существует два фундаментальных подхода к организации ядра сети: **коммутация каналов и коммутация пакетов**. При коммутации каналов происходит резервирование на время сеанса связи необходимых ресурсов (буферов, диапазонов частот) на всем сетевом пути. При коммутации пакетов ресурсы запрашиваются при необходимости и выделяются по требованию. Иногда несколько сообщений могут пытаться использовать линию связи одновременно, поэтому возникает необходимость в организации очередей сообщений.

Современный Интернет, является типичной сетью с коммутацией пакетов. Как правило, при передаче пакет проходит через множество каналов, однако никакого резервирования частотных полос при этом не происходит. В случае перегруженности какого-либо канала пакет будет вынужден ждать в очереди его освобождения. Таким образом, хотя с точки зрения быстродействия Интернет пытается доставлять пакеты *с максимальными усилиями,* время доставки не гарантировано. Не каждую телекоммуникационную сеть можно однозначно отнести к сетям с коммутацией каналов или сетям с коммутацией пакетов. Так, например, сети, использующие режим асинхронной передачи (Asynchronous Transfer Mode, ATM), организованы таким образом, что резервирование ресурсов в них сочетается с организацией очередей сообщений. Тем не менее, разделение компьютерных сетей на сети с коммутацией каналов и коммутацией пакетов является удобной «отправной точкой» для изучения телекоммуникационных технологий.

У нас появилось сразу три вопроса: что такое информационный поток? На чём основан механизм коммутации пакетов? Как возможно пакеты передавать через сеть с коммутацией каналов? Рассмотрим последовательно эти три понятия.

## 4.2. Информационный поток - определение

Через один транзитный узел может проходить несколько маршрутов. Например, через узел 5 (см.рис.4.1) проходят, все данные, направляемые узлом 4 каждому из остальных узлов, а также все данные, поступающие в узлы 3,4 и 10. Транзитный узел должен уметь распознавать поступающие на него потоки данных, для того чтобы обеспечивать передачу каждого из них именно на тот свой интерфейс, который ведет к нужному узлу.

Информационным потоком, или потоком данных, называют непрерывную последовательность данных, объединенных набором общих признаков, выделяющих эти данные из общего сетевого трафика.

Например, как поток можно определить все данные, поступающие от одного компьютера; объединяющий признак - адрес источника. Эти же данные можно представить как совокупность нескольких подпотоков, признак - адрес назначения. Наконец, каждый из этих подпотоков, в свою очередь, можно разделить на более мелкие подпотоки, созданные разными сетевыми приложениями — электронной почтой, программой копирования файлов, веб-сервером. Данные, образующие поток, могут быть представлены в виде различных информационных единиц данных — пакетов, кадров или ячеек.

При коммутации обязательным признаком потока является адрес назначения данных. На основании адреса назначения весь поток данных, входящих в транзитный узел разделяется на подпотоки, каждый из которых передается на интерфейс, соответствующий маршруту продвижения данных. Адреса источника и назначения определяют поток для пары соответствующих конечных узлов.

## 4.3. Коммутация пакетов

В компьютерных сетях большие по объёму сообщения разбиваются на более мелкие фрагменты – пакеты. При передаче пакет проходит через последовательность линий связи ЛС и маршрутизаторов. Маршрутизаторы используют механизм передачи с промежуточным накоплением – пакет сначала полностью принимается и записывается в буфер, затем передаётся в ЛС



(см.рис.4.2)[37]. В маршрутизаторах возникает задержка накопления, которая пропорциональна длине пакета:

$$Тзн=L/R$$

где L – длина пакета бит, R – скорость выходной ЛС бит/с

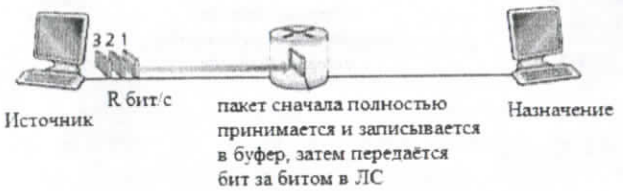



Рис.4.2. Накопление и продвижение пакетов при пакетной коммутации

Маршрутизатор имеет много входных и выходных ЛС. Каждая ЛС имеет выходной буфер (выходная очередь) ограниченного размера. Т.к. размеры буферов ограничены, может возникнуть ситуация, когда свободного места в буфере будет недостаточно для помещения нового пакета. В этом случае произойдёт потеря пакета – будет утрачен либо новый пакет, либо один из пакетов, находящихся в очереди.

Рассмотрим структуру простой сети с коммутацией пакетов (см.рис.4.3)[38]. Хосты A,B посылают одновременно пакеты к хосту E, связь хостов A и B с первым маршрутизатором осуществляется с помощью ЛС Ethernet со скоростью 10Мбит/с. маршрутизатор направляет пакеты в ЛС со скоростью 1,5Мбит/с. Если ЛС перегружена пакеты ожидают её освобождения в очереди.

Посмотрим, что произойдёт, если A и B одновременно посылают пакеты. Между хостами нет синхронизации, нельзя заранее предсказать порядок передачи пакетов, такой метод называется статическое мультиплексирование.

---

[37] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

[38] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

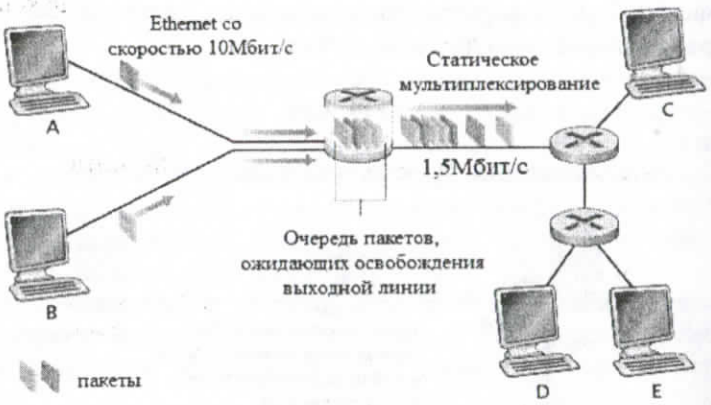



Рис.4.3. Структура простой сети с коммутацией пакетов

Время пересылки пакета между хостами равно:

$$Tп=Q*L/R$$

где L – длина пакета бит, R – скорость выходной ЛС бит/с, Q – число ЛС между хостами.

Пакеты поступают в сеть *без предварительного резервирования ЛС*, со скоростью с которой их генерирует источник. Предполагается, что сеть с коммутацией пакетов, в отличие от сети с коммутацией каналов, всегда готова принять пакет от конечного узла.

Коммутация пакетов не позволяет качественно обслуживать приложения реального времени, такие как телефония, видеовызов, конференц-связь, но позволяет эффективно организовывает разделение пропускной способности ЛС.

### 4.4. Обработка пакета в маршрутизаторе

В состав пакета входят заголовок, поле данных, концевик. Заголовок - поле, размещаемое в начале пакета, содержит адрес назначения и другую вспомогательную информацию (длина поля данных, контрольная сумма и др.), используемую для доставки пакета адресату. Концевик - поле, размещаемое в конце пакета, содержит контрольную сумму, которая позволяет проверить, была ли искажена



информация при передаче через сеть или нет. Каждый пакет обрабатывается коммутатором *независимо* от других пакетов, составляющих сетевой трафик. В зависимости от технологии пакеты могут иметь фиксированную или переменную длину, может меняться состав информации, размещенной в заголовках пакетов, например:

- технология ATM пакеты (ячейки) имеют фиксированную длину,
- в Ethernet установлены лишь мин и макс возможные размеры пакетов (кадров).

На рис.4.4 приведена структурная схема маршрутизатора[39]. Каждый пакет последовательно бит за битом помещается во входной буфер (см.рис.4.5)[40]. Маршрутизатор не может принять решения о продвижении пакета, не имея в своей памяти всего пакета. Маршрутизатор проверяет контрольную сумму, и только если она говорит о том, что данные пакета не искажены, начинает обрабатывать пакет и по адресу назначения определяет следующий маршрутизатор.


Рис.4.4. Архитектура маршрутизатора

Буферы нужны для выполнения следующих функций:

- для согласования скоростей передачи данных в ЛС, подключенных к интерфейсам маршрутизатора. Если скорость поступления пакетов из одной ЛС превышает пропускную способность

[39] [40] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

выходной ЛС, то во избежание потерь пакетов на интерфейсе организовываетя выходная очередь;
- для согласования скорости поступления пакетов со скоростью их коммутации. Если коммутирующий блок не успевает обрабатывать пакеты (анализировать заголовки и перебрасывать пакеты на нужный интерфейс), то на интерфейсах коммутатора возникают входные очереди (см.рис.4.6)[41].

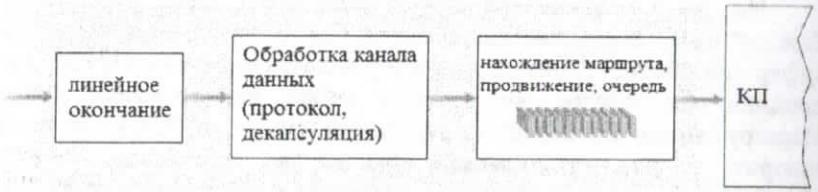



Рис.4.5. Обработка входного порта

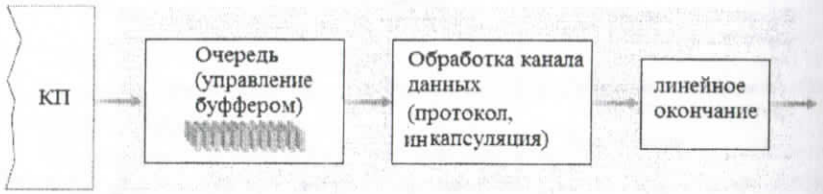



Рис.4.6. Обработка выходного порта

Существует 3 метода продвижения пакетов в пакетном коммутаторе
- дейтаграммная передача;
- передача с установлением логического соединения;
- передача с установлением виртуального канала.

### 4.4.1. Дейтаграммная передача

Пакеты передаются от одного узла сети к другому *независимо* друг от друга на основании одних и тех же правил (см.рис.4.7)[42].

[41] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013
[42] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



Процедура обработки пакета определяется только значениями параметров, которые он несет в себе, и текущим состоянием сети. Информация об *уже переданных пакетах* сетью не хранится и в ходе обработки очередного пакета во внимание не принимается. Каждый отдельный пакет рассматривается сетью как совершенно независимая единица передачи – **дейтаграмма.** Решение о продвижении пакета принимается на основе таблицы коммутации (маршрутизации), ставящей в соответствие адресам назначения пакетов информацию, однозначно определяющую следующий по маршруту транзитный (или конечный) узел.

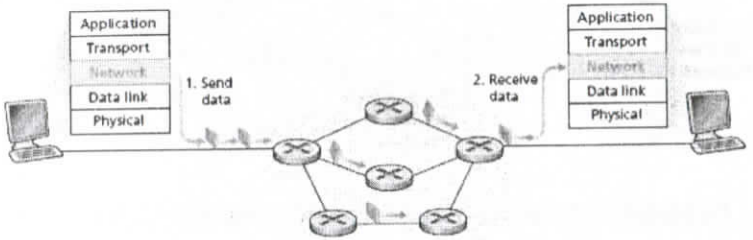



Рис.4.7. Дейтаграммная сеть

### 4.4.2. Передача с установлением логического соединения

Передача с установлением логического соединения – означает, что между хостом-отправителем и хостом-получателем существует процедура согласования двумя конечными узлами сети некоторых параметров процесса обмена пакетами. Она заключается в следующем (см.рис.4.8)[43].

1. Узел-инициатор соединения отправляет узлу-получателю служебный пакет с предложением установить соединение.
2. Если узел-получатель согласен с этим, то он посылает в ответ другой служебный пакет, подтверждающий установление соединения и предлагающий некоторые параметры, которые будут

[43] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013
В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010

использоваться в рамках данного логического соединения (идентификатор соединения, количество кадров, которые можно отправить без получения подтверждения и т.п.)


Рис.4.8. Передача с установлением логического соединения

3. Узел-инициатор соединения может закончить процесс установления соединения отправкой третьего служебного пакета, в котором сообщит, что предложенные параметры ему подходят.

### 4.4.3. Передача с установлением виртуального канала

Передача с установлением виртуального канала – частный случай логического соединения, в котором жестко определен *маршрут* для всех пакетов. Все пакеты, передаваемые в рамках данного соединения, должны проходить по одному и тому же закрепленному за этим соединением пути (см.рис.4.9)[44]. Единственный заранее проложенный фиксированный маршрут, соединяющий конечные узлы в сети с коммутацией пакетов, называют виртуальным каналом (virtual circuit или virtual channel VC). Виртуальные каналы прокладываются для *устойчивых* информационных потоков. Для выделения потока данных из общего трафика каждый пакет этого потока помечается специальным видом признака — меткой.

[44] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



Процедура передачи с установлением виртуального канала включает следующие шаги:

1. Прокладка виртуального канала - отправка из узла-источника специального пакета — запроса на установление соединения (адрес назначения и метка потока, для которого прокладывается этот виртуальный канал).

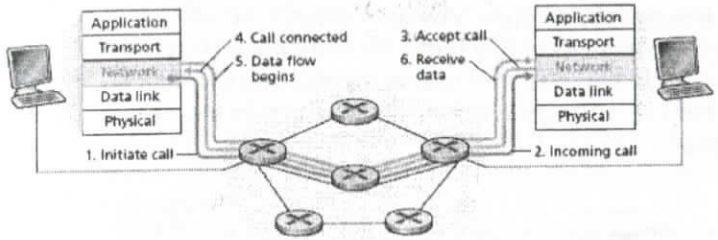



Рис.4.9. Передача с установлением виртуального канала

2. Запрос, проходя по сети, формирует новую запись в каждом из коммутаторов, расположенных на пути от отправителя до получателя, которая говорит о том, каким образом коммутатор должен обслуживать пакет, имеющий заданную метку.
3. Образованный виртуальный канал идентифицируется той же меткой.
4. После прокладки виртуального канала сеть может передавать по нему соответствующий поток данных.

При поступлении пакета на входной интерфейс коммутатор читает значение метки из заголовка пакета и просматривает свою таблицу коммутации, по которой определяет, на какой выходной порт передать пакет.

## 4.5. Коммутация каналов

Примером сетей с коммутацией каналов являются телефонные сети. Рассмотрим, что происходит, когда у одного абонента возникает необходимость передать информацию другому абоненту. Перед тем как начать разговор, нужно установить соединение между принимающей и передающей сторонами. В отличие от логического

соединения, рассматриваемое соединение является «настоящим» (реальным), то есть все каналы, лежащие на пути между абонентами, находятся в состоянии связи. На языке телефонии такое соединение называется **коммутацией**. При коммутации на все время соединения устанавливается постоянная частота передачи. Это возможно благодаря тому, что в телефонных сетях используется стандартная полоса частот.

Кратко рассмотрим коммутируемые телефонные сети. Это поможет лучше понять причины, по которым в Интернете используется коммутация пакетов, а не традиционная коммутация каналов.

На рис.4.10 приведена типичная структура сети с коммутацией каналов[45].

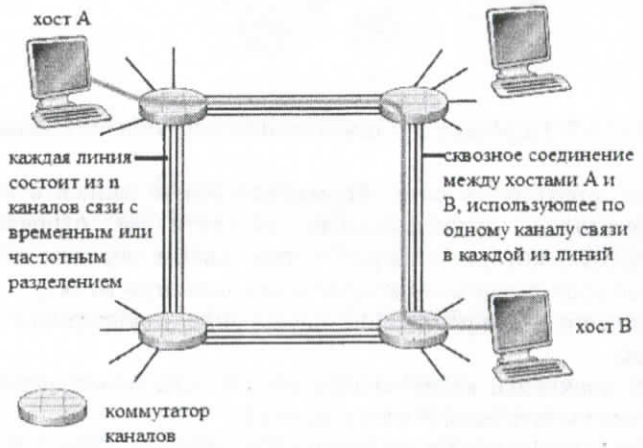



Рис.4.10. Простейшая сеть с коммутацией каналов

В этой сети четыре коммутатора соединены между собой линиями связи. Каждая из линий способна одновременно поддерживать n каналов связи. Хосты (персональные компьютеры, рабочие станции и т.п.) напрямую соединены с одним из коммутаторов. Между парами хостов устанавливается выделенное сквозное соединение (соединения «конференция», позволяющие общаться одновременно множеству абонентов, в подобных сетях

[45] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



также возможны, но мы их не рассматриваем). Таким образом, чтобы хост А имел возможность передавать пакеты хосту В, необходимо зарезервировать одну полосу частот на каждой из двух линий связи, соединяющих хосты А и В. Поскольку каждая линия связи способна поддерживать одновременно n каналов связи, ширина полосы канала связи составляет 1 */n* часть от полосы пропускания линии связи.

Рассмотрим процесс мультиплексирования в сетях с коммутацией каналов. Каждый канал связи в линии связи организовывается при помощи **частотного** либо **временного разделения**. В первом случае каждому каналу связи отводится определенная полоса частот, которая не изменяется в течение всего сеанса связи. Например, для телефонных сетей типичной шириной полосы пропускания является 4кГц. Радиостанции, работающие в FM-режиме, также используют принцип частотного разделения.

В настоящее время в телефонии наблюдается тенденция замены частотного разделения каналов ЧРК (FDM в английской терминологии) временным разделением каналов ВРК, большинство технологически развитых телефонных сетей уже использует принцип ВРК (TDM в английской терминологии). Суть ВРК заключается в следующем: время разбивается на равные промежутки, называемые кадрами, а каждый кадр делится на фиксированное число слотов. Выделение канала связи заключается в закреплении за парой абонентов одного временного слота в каждом кадре. Внутри этого слота происходит монопольная передача пакетов между абонентами по линии связи.

На рис.4.11 показаны схемы функционирования линии связи, поддерживающей четыре канала, для случаев частотного и временного разделения[46]. При частотном разделении полоса пропускания линии связи делится на 4 равные диапазона по 4кГц. При временном разделении время делится на кадры, в каждом из которых имеются 4 слота; за каждым каналом связи закреплен один из этих слотов. Скорость передачи для временного разделения равна произведению частоты следования кадров и числа битов внутри каждого слота. Например, если частота следования кадров составляет 8000 кадров в секунду, а слот включает 8бит, то скорость передачи по каналу связи будет составлять 64кбит/с.

[46] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

Сторонники технологии коммутации пакетов всегда обращали внимание на серьезный недостаток сетей с коммутацией каналов, заключающийся в том, что выделенные каналы связи нельзя освободить в периоды *простоя*. Например, если во время телефонного разговора собеседники молчат (не передают информацию), то выделенный для них канал нельзя «отобрать» и использовать для других соединений. Представьте себе радиолога, которому необходим удаленный доступ к рентгеновским снимкам. Если этот доступ осуществляется при помощи коммутации каналов, то радиолог сначала устанавливает соединение, получает снимок, просматривает его, а затем запрашивает новый снимок. Все периоды времени, когда он занимается изучением снимков, являются простоями с точки зрения передачи информации по каналу связи.

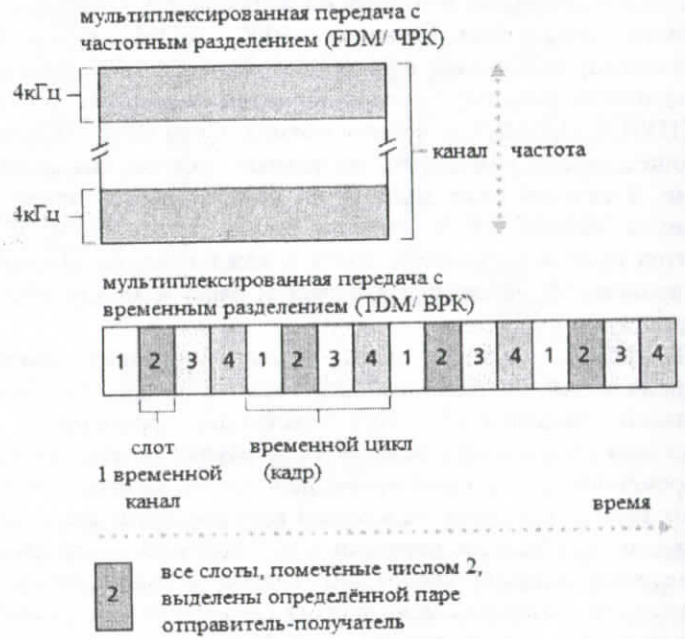



Рис.4.11. При ЧРК канал связи непрерывно использует свою частотную полосу, а при ВРК – всю полосу пропускания ЛС в отведённые ему временные слоты



Другой причиной, по которой коммутация каналов вызывает вполне обоснованную критику, является необходимость в сложном сигнальном оборудовании для управления коммутациями и выделения частотных полос каналам связи.

Перед тем как завершить разговор о сетях с коммутацией каналов, давайте рассмотрим численный пример, наглядно иллюстрирующий суть этой технологии. Пусть нам необходимо передать файл размером 640000бит от хоста А хосту В методом коммутации каналов. Сколько времени займет передача? Предположим, что все линии связи в сети одинаковы, используют принцип временного разделения, при этом число слотов кадра равно 24, а скорость передачи по линии составляет 1,536Мбит/с. Предположим также, что временные затраты на установление соединения хоста А с сетью равны 0,5 с. Итак, поскольку скорость линии связи поровну «распределяется» между всеми каналами связи, скорость передачи по каналу связи составляет (1,536Мбит/с) / 24 = 64кбит/с. Теперь мы можем рассчитать время передачи файла по каналу связи: 640000бит / (64кбит/с) = 10с. Учитывая затраты хоста А на установление соединения, получаем полное время передачи файла: 10с + 0,5 с = 10,5 с. В первом приближении время передачи не зависит от числа линий связи: его можно считать равным 10с и в случае одной линии, и в случае 100 линий.

### 4.5.1. Пример мультиплексирования – структура первичного цифрового потока Е1

В результате мультиплексирования формируется групповой цифровой сигнал, который позволяет организовывать большое число независимых каналов, использующихся для передачи кодовых групп от определенного числа абонентов.

Коммутаторы каналов транспортной сети строятся на различных системах передачи СП, образуя транспортную сеть. Структура транспортной сети предопределяет объединение и разделение потоков передаваемой информации, поэтому используемые на ней СП строятся по **иерархическому принципу**. Для цифровых систем передачи ЦСП – число каналов ЦСП, соответствующее данной ступени иерархии, больше числа каналов ЦСП предыдущей ступени в целое число раз.

ЦСП, соответствующая 1-ой ступени иерархии, называется первичной, она осуществляет прямое преобразование относительно небольшого числа первичных сигналов в первичный цифровой поток. ЦСП 2-ой ступени иерархии объединяют определенное число первичных потоков во вторичный цифровой поток и т.д.

Первичный сигнал для всех типов ЦСП – цифровой поток 64кбит/с, называемый основным цифровым каналом. Для объединения сигналов 64кбит/с в групповые высокоскоростные цифровые сигналы используется принцип ВРК.

ЦСП, использующие только основной цифровой канал 64кбит/с, называются узкополосными и имеют три разновидности (стандарта):

- европейский на основе первичного цифрового потока E1,
- североамериканский основе первичного цифрового потока T1,
- японский основе первичного цифрового потока J1.

В табл.4.1 приведены характеристики данных стандартов.

Таблица 4.1.

Характеристики данных стандартов узкополосных ЦСП

| Уровень ЦСП | Европа | | Северная Америка | | Япония | |
|---|---|---|---|---|---|---|
| | Скорость Мбит/с | Коэффициент мультиплексирования | Скорость Мбит/с | Коэффициент мультиплексирования | Скорость Мбит/с | Коэффициент мультиплексирования |
| | 2,048 | 30 | 1,544 | 24 | 1,544 | 24 |
| | 8,448 | 4 | 6,312 | 4 | 6,312 | 4 |
| | 34,368 | 4 | 44,736 | 7 | 32,064 | 3 |
| | 139,264 | 4 | 274,176 | 6 | 97,728 | 4 |

В Узбекистане цифровые системы передачи используют европейский стандарт на основе первичного цифрового потока E1, иначе называемый СП ИКМ 30/32. Рассмотрим структуру и параметры потока E1 (СП ИКМ 30/32). Структура потока E1 приведена на рис.4.12. Для управления поток E1 использует логическое деление группового цифрового сигнала на сверхциклы. В одном сверхцикле передаются кодовые группы 16-ти циклов передачи. В каждом цикле – 32 канальных интервала с 8-ми разрядными кодовыми словами в каждом канале. Из 32 каналов – 30 речевых и 2 служебных (0 и 16).



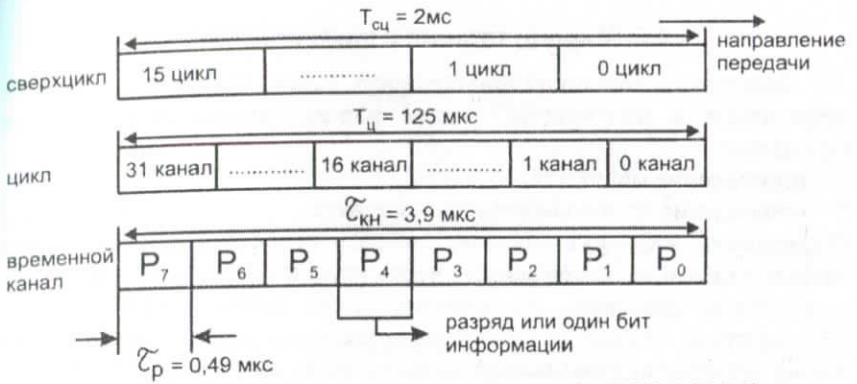



Рис.4.12. Структура потока E1 (тракта ИКМ 30/32)

ИКМ 30/32 используется для группообразования 30 речевых канальных интервалов (с 1-15, с 17-31) в одном цикле передачи совместно с каналом синхронизации (0-й) и каналом сигнализации (16). При этом частота дискретизации $f_д = 8$ кГц, тактовая частота $f_{такт} = 2048$ кГц. В табл.4.2 приведены характеристики потока E1.

Таблица 4.2.

Параметры системы E1:

| | | |
|---|---|---|
| 1. | Скорость потока, кбит/с | 2048 |
| 2. | Длительность цикла, мкс | 125 |
| 3. | Число каналов в цикле передачи | 32 |
| 4. | Число символов в одном временном канале | 8 |
| 5. | Число каналов ТЧ | 30 |
| 6. | Диапазон канала ТЧ, Гц | 300-3400 |
| 7. | Длительность сверхцикла, мс | 2 |
| 8. | Число циклов в сверхцикле | 16 |
| 9. | Число сигнальных каналов на один канал ТЧ | 2-4 |
| 10. | Частота дискретизации, кГц | 8 |
| 11. | Число уровней квантования | 256 |
| 12. | Закон квантования | А-закон А-87,6 |
| 13. | Размещение сигналов управления и взаимодействия | 16 канал |
| 14. | Цикловая синхронизация | 0 канал |

## 4.6. Маршрутизация в интернет сетях

Маршрут – это последовательность узлов, лежащих на пути от отправителя к получателю. Задача маршрутизации включает две подзадачи:

1. определение маршрута;
2. оповещение сети о выбранном маршруте.

**Определить маршрут** означает выбрать последовательность транзитных узлов и их интерфейсов, через которые надо передавать данные, чтобы доставить их адресату. Если между парой взаимодействующих сетевых интерфейсов существует множество путей, то выбирают один **оптимальный** по некоторому критерию маршрут.

Задача выбора пути пакета от хоста-источника к хосту-приемнику, очевидно, сводится к задаче выбора пути пакета от маршрутизатора-источника к маршрутизатору-приемнику.

Сердцевиной любого протокола маршрутизации является алгоритм, определяющий путь пакета от маршрутизатора-источника к маршрутизатору-приемнику (**алгоритм маршрутизации**). Задача алгоритма маршрутизации проста: для заданного множества маршрутизаторов и линий, соединяющих маршрутизаторы, алгоритм маршрутизации находит «оптимальный» путь от маршрутизатора-источника к маршрутизатору-приемнику. Как правило, «оптимальный» означает путь с «минимальной стоимостью». Мы увидим, однако, что на практике в игру часто вступают такие стратегические соображения, как вопросы безопасности.

Для формулирования алгоритмов маршрутизации сеть рассматривается как граф (рис.4.13)[47]. Узлы графа представляют маршрутизаторы — точки, в которых принимаются решения о продвижении пакетов, — а линии (в соответствии с терминологией теории графов называемые «ребрами»), соединяющие эти узлы, представляют физические линии между маршрутизаторами. Каждой линии связи соответствует некоторое значение, представляющее «стоимость» пересылки пакета по этой линии. Стоимость может зависеть от физической длины линии (например, стоимость передачи кадра по трансокеанскому кабелю может быть выше, чем по короткому кабелю, проложенному по суше), скорости передачи данных по линии или финансовой стоимости линии.

[47] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



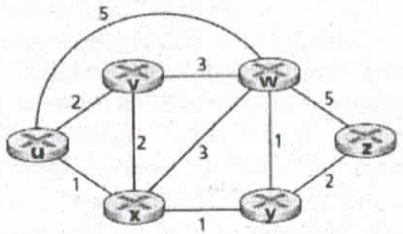



Рис.4.13. Абстрактная модель сети

При рассмотрении сети в виде графа для решения задачи определения пути от отправителя к получателю с минимальной стоимостью необходимо найти последовательность линий такую, что:

- первая линия пути соединена с источником;
- последняя линия пути соединена с адресатом;
- для всех $i$ линии с номерами $i$ и $i$ - 1 соединены с одним и тем же узлом;
- для *пути с минимальной стоимостью* сумма стоимостей всех линий пути является минимальной по всем возможным путям между отправителем и получателем.

Например, на рис.4.13 путь с минимальной стоимостью между узлами $A$ (отправителем) и $C$ (получателем) представляет собой маршрут $ADEC$.

Все алгоритмы маршрутизации можно разбить на два класса: глобальные и децентрализованные.

- *Глобальный алгоритм маршрутизации* находит путь с наименьшей стоимостью от отправителя до получателя с помощью полной информации о сети. Сами вычисления могут производиться на каком-либо одном компьютере или тиражироваться в разных местах. Однако ключевой особенностью здесь является то, что глобальный алгоритм обладает *полной* информацией о топологии сети и стоимости линий. Примером является «Алгоритм маршрутизации, основанный на состояниях линий».
- В *децентрализованном алгоритме маршрутизации* вычисление пути с наименьшей стоимостью выполняется распределенным

образом. Ни один узел не обладает полной информацией о стоимости всех линий сети. Изначально каждому узлу известна только стоимость напрямую присоединенных к нему линий. Затем, путем итерационных вычислений и обмена информацией с соседними узлами (то есть узлами, находящимися на противоположных концах напрямую присоединенных к нему линий) узел постепенно определяет путь с наименьшей стоимостью до получателя или до группы получателей. Примером является «Дистанционно-векторный алгоритм».

Кроме того, все алгоритмы маршрутизации можно разделить на *статические* и *динамические.* В статическом алгоритме маршрутизации маршруты изменяются со временем очень медленно, часто в результате вмешательства человека (например, администратор сети может вручную отредактировать таблицу продвижения данных маршрутизатора). Динамический алгоритм может либо запускаться периодически, либо в ответ на изменения топологии или стоимости линий.

Третий способ классификации алгоритмов маршрутизации определяется по тому, чувствителен ли алгоритм к перегрузке. В *чувствительном к перегрузке алгоритме* стоимости линий динамически изменяются, отражая текущий уровень перегрузки в соответствующей линии. Если с временно перегруженной линией ассоциируется высокая стоимость, алгоритм маршрутизации будет стараться выбирать маршруты в обход перегруженной линии. Сегодня в Интернете применяются алгоритмы, нечувствительные к перегрузке (RIP, OSPF и BGP), так как стоимость линии, как правило, не отражает ее текущего (или недавнего) уровня перегрузки.

В Интернете, как правило, используются только два типа алгоритмов маршрутизации: динамический глобальный алгоритм, основанный на состояниях линий, и динамический децентрализованный дистанционно-векторный алгоритм.

### Контрольные вопросы

1. Что такое коммутация? Дайте определение.
2. Что такое маршрут?
3. Что входит в состав задачи коммутации ?
4. Что такое Информационный поток? Дайте определение.
5. Что входит в состав задачи маршрутизации



6. Поясните принцип работы коммутации пакетов?
7. Из каких функциональных блоков состоит маршрутизатор?
8. Какими методами обрабатываются пакеты в маршрутизаторе?
9. На чём базируется коммутация каналов?
10. Что определяет алгоритм маршрутизации? Какова его задача?
11. По каким принципам классифицируются алгоритмы маршрутизации?

функциональностью, то есть службами, предоставляющими услуги пассажирам. Ниже билетного уровня пассажир проходит через все этапы обслуживания от получения билета до приема жалобы, ниже багажного уровня — все этапы от проверки и сдачи багажа до его получения, и т.д. При этом на багажном уровне обслуживаются лишь те пассажиры, которые прошли обслуживание на билетном уровне. То же самое справедливо и в отношении остальных уровней. Таким образом, обслуживание на каждом из уровней производится путем выполнения функций, относящихся к этому уровню, с использованием результатов обслуживания на всех предыдущих уровнях.

Многоуровневая структура позволяет детально оценивать элементы большой и сложной системы. С использованием многоуровневой структуры легче модифицировать функции системы — для этого лишь нужно внести изменения в соответствующий уровень, при этом структурно-функциональная организация системы останется прежней. Так, например, усовершенствование системы регистрации будет сведено к внутренним изменениям регистрационного уровня, что никак не отразится на его функциях и не изменит структуру в целом.

## 5.2. Стек протоколов Интернета

Теперь давайте рассмотрим организацию сетевых протоколов. Протоколы и все сетевое программное и аппаратное обеспечение организованы в виде *уровней*. Каждый протокол относится к определенному уровню сетевой коммуникационной модели.

Поддержка протоколов может быть аппаратной, программной или смешанной. Протоколы прикладного уровня, такие как HTTP и SMTP, а также протоколы транспортного уровня практически всегда поддерживаются программно. Напротив, протоколы физического и канального уровней, тесно связанные со средой передачи данных, поддерживаются аппаратно сетевой интерфейсной картой (например, Ethernet, Wi-Fi). Сетевой уровень, находящийся в центре коммуникационной модели, может поддерживаться как аппаратно, так и программно. Далее даны характеристики каждого из пяти уровней коммуникационной модели Интернета.

Протоколы *распределены* между сетевыми компонентами, включающими оконечные системы и маршрутизаторы, подобно тому



как функции обслуживания пассажиров распределены между аэропортами.

Совокупность протоколов всех уровней коммуникационной модели называется *стеком протоколов*.

Коммуникационная модель Интернета состоит из пяти уровней: физического, канального, сетевого, транспортного и прикладного (см.рис.5.3).

### 5.2.1. Прикладной уровень

Прикладной уровень предназначен для поддержки сетевых приложений. Имеется множество протоколов прикладного уровня, из которых наиболее важными являются HTTP (для путешествий по web-страницам), SMTP (для электронной почты) и FTP (для обмена файлами).

Протоколы прикладного уровня распределены по оконечным системам, каждое приложение на оконечной системе использует протокол для обмена пакетами информации с другой оконечной системой. Единицы обмена прикладного уровня (пакеты информации) называются *сообщениями*.

### 5.2.2. Транспортный уровень

Главная функция транспортного уровня заключается в передаче сообщений прикладного уровня между конечными точками (клиентом и сервером). В Интернете существуют два транспортных протокола: TCP и UDP. Протокол TCP обеспечивает передачу с установлением логического соединения, то есть надежную передачу с контролем переполнения. Протокол TCP производит разбиение длинных сообщений на более короткие и контролирует перегрузку. Протокол UDP обеспечивает передачу сообщений без установления логического соединения, то есть ненадежный вид связи, где допускаются искажения и потери данных. Единицы обмена транспортного уровня называются *сегментами*.


Рис.5.3. Стек протоколов Интернета и модель OSI



### 5.2.3. Сетевой уровень

Сетевой уровень обеспечивает передачу дейтаграмм между двумя хостами. Протокол транспортного уровня Интернет (TCP или UDP) передает сегмент и адрес назначения протоколу IP сетевого уровня, а протокол IP сетевого уровня доставляет сегмент конечному хосту и передает его обратно транспортному уровню. Сетевой уровень содержит протокол IP, который определяет поля дейтаграммы и интерпретацию их содержимого маршрутизаторами и оконечными системами. Сетевой уровень содержит также многочисленные протоколы маршрутизации, предназначенные для определения путей дейтаграмм от отправителя до адресата. Несмотря на функциональные различия между протоколом IP и протоколами маршрутизации, их обычно объединяют под общим именем IP, подчеркивая этим их связующую роль в организации глобальной Сети.

### 5.2.4. Канальный уровень

Сетевой уровень обеспечивает передачу пакета через серию маршрутизаторов между оконечными системами. Для перемещения пакета (дейтаграммы) от одного узла к другому сетевой уровень прибегает к службам канального уровня. Основная функция канального уровня заключается в передаче дейтаграмм между узлами на маршруте.

Канальный уровень использует специальный протокол, ориентированный на используемую линию связи. Иногда протоколы канального уровня обеспечивают надежную передачу между узлами. Обратите внимание на различие надежной передачи на транспортном и канальном уровнях: протокол TCP обеспечивает надежность на всем пути следования сообщения, а протокол канального уровня — лишь между парой узлов. К протоколам канального уровня относятся Ethernet, Wi-Fi. Например, дейтаграмма может обрабатываться протоколом Ethernet на одном участке и протоколом PPP на другом участке. Поскольку путь от отправителя до адресата обычно состоит из цепочки разнородных линий связи, передача дейтаграммы может осуществляться различными канальными протоколами. Единицы обмена канального уровня мы назовем *кадрами.*

### 5.2.5. Физический уровень

Если назначением канального уровня является передача кадров между соседними узлами сети, то физический уровень обеспечивает передачу между узлами отдельных битов информации. Протоколы физического уровня также напрямую зависят от использующейся линии связи (медной витой пары, одномодового оптоволокна и т.п.). Технология Ethernet поддерживает множество протоколов физического уровня, предназначенных для поддержки витой пары, коаксиального кабеля, оптоволоконного кабеля и некоторых других видов линий. В каждой из линий связи механизмы передачи бита различны.

## 5.3. Эталонная модель взаимодействия открытых систем ВОС (OSI)

Обсуждая стек интернет-протоколов необходимо отметить, что это не единственная реализация стека протоколов. В 70г.г. XXв. Международная организация по стандартизации (ISO) предложила для организации компьютерных сетей 7-уровневую модель, называемую моделью взаимодействия открытых систем ВОС (Open System Interconnection OSI).

Одна из проблем развития связи заключается в обеспечении совместимости средств связи от разных производителей. Для решения этой проблемы разработаны международные рекомендации и стандарты. Эталонная модель взаимодействия открытых систем ВОС, по английски называемая моделью OSI используется для описания функциональной архитектуры средств связи.

Модель OSI состоит из 7 уровней (см.рис.5.4): уровень приложений, уровень представлений, сеансовый уровень, транспортный уровень, Сетевой уровень, канальный уровень, физический уровень. Функции пяти из этих уровней идентичны функциям уровней с такими же названиями интернет стека. Рассмотрим два дополнительных уровня модели OSI – уровень представлений, сеансовый уровень. Назначение уровня представлений предоставить сервисы, которые позволят коммуникативным приложениям интернет производить обмен данными. Эти сервисы включают – компрессию данных, шифрование данных. Сеансовый уровень обеспечивает разграничение и синхронизацию данных при обмене, включая схемы проверки достоверности передачи данных и схемы восстановления данных.



Прикладной уровень обеспечивает управление взаимодействием прикладных процессов, протокол прикладного уровня выполняет управление вычислительными процессами, доступом к внешним устройствам, административное управление сетью.

Уровень представлений производит перекодировку сообщения, поступившего с седьмого уровня, в единое кодовое представление этого сообщения, принятого в сети связи, протокол представительного уровня отвечает за доступ к файлам данных и командным файлам (локальным), преобразование данных в требуемый формат, подготовка эмуляторов программ к работе.


Рис.5.4. Уровни модели OSI

Сеансовый уровень предназначен для открытия сеанса связи между удалёнными процессами пользователя, протокол сеансового уровня выполняет формирование каталога сетевых процессов, установление логического соединения с удаленными процессами, завершение сеанса связи.

Транспортный уровень обеспечивает разделение сообщения на пакеты, которые имеют ограниченный размер, протокол транспортного уровня отвечает за передачу файлов данных и доступ к удаленным файлам, передача и удалённое управление командными файлами, фрагментация и сборка передаваемых сообщений.

Сетевой уровень производит выбор маршрута в сети с использованием специальных пакетов, протокол сетевого уровня отвечает за установление и закрытие логических соединений через коммуникационную подсеть, управление потоками данных и маршрутами движения сообщений (пакетов).

Канальный уровень формирует в кадры пакеты, поступающие с сетевого уровня, протокол канального уровня отвечает за управление передачей и приёмом сообщений (кадров), контроль ошибок, формирование сообщений (кадров).

Физический уровень осуществляет побитовую передачу кадров по линии связи, протокол физического уровня отвечает за установление и разъединение физических соединений, управление сигнализацией и тактированием.

В данной модели более низкий уровень всегда предоставляет услуги более высокому уровню. Взаимодействие между разными уровнями осуществляется в рамках одной системы. Взаимодействие между одинаковыми уровнями означает взаимодействие между системами. Сообщения, используемые для взаимодействия, называются протоколами. Протоколы уровней 4-7 это протоколы верхнего уровня. Протоколы уровня 1-3 протоколы нижнего уровня.

### 5.4. Инкапсуляция данных

На рис.5.5 показан физический путь, который данные проходят между оконечными системами, включая прохождение через все уровни (вверх и вниз) протокольного стека и обработку в маршрутизаторах[50]. Наиболее важными сетевыми устройствами являются оконечные системы и коммутаторы (маршрутизаторы и коммутаторы 2 уровня). Как и оконечные системы, мосты и маршрутизаторы поддерживают многоуровневую структуру сети, однако они обслуживают лишь нижние уровни. Как можно видеть на рис.5.5, мосты обслуживают только физический и канальный уровни, а маршрутизаторы — физический, канальный и сетевой уровни. Это объясняется тем, что маршрутизаторы способны поддерживать протокол IP, в то время как мосты не обладают такой возможностью. Мосты распознают не IP-адреса, а лишь адреса канального уровня. Хосты обслуживают все пять сетевых уровней; это говорит о том, что архитектура Интернета передаёт большую часть своей сложности «на плечи» оконечных систем.

[50] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



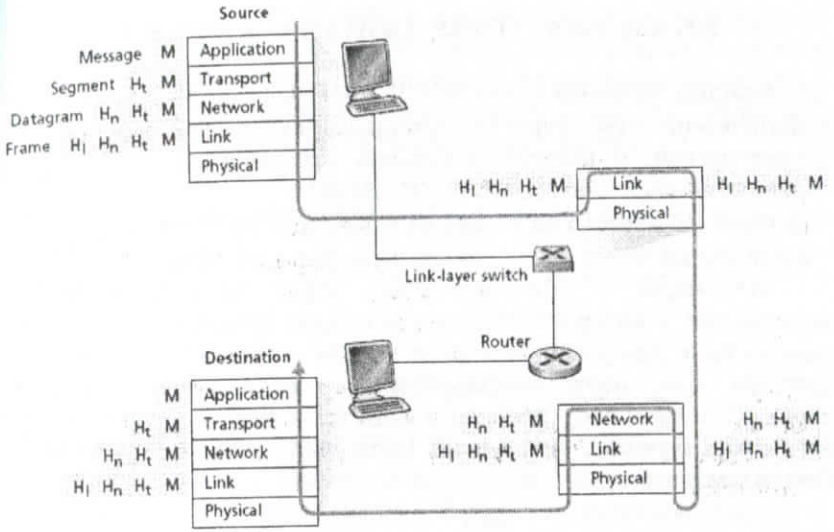



Рис.5.5. Хосты, мосты, маршрутизаторы и поддерживаемые ими уровни коммуникационной модели

Рис.5.5 иллюстрирует понятие «инкапсуляции» данных. Хост-отправитель создаёт сообщение прикладного уровня M, которое передаётся на транспортный уровень. Транспортный уровень добавляет к сообщению дополнительную информацию, называемую заголовком транспортного уровня Ht, которая будет использоваться принимающей стороной транспортного уровня. сообщение прикладного уровня M и заголовок транспортного уровня Ht вместе образуют сегмент транспортного уровня. Транспортный уровень инкапсулировал в себя сообщение прикладного уровня. Сегмент транспортного уровня поступает на сетевой уровень, который добавляет информацию заголовка сетевого уровня Hn, такую как адрес источника и назначения, создавая дейтаграмму сетевого уровня. Дейтаграмма поступает на канальный уровень, который добавляет информацию заголовка канального уровня, создавая кадр канального уровня. Мы можем видеть, что на каждом уровне пакет состоит из 2 частей – заголовка и поля данных. В качестве поля данных выступают данные верхнего уровня.

## 5.5. Адресация TCP/IP. Типы адресов в IP-сетях

Каждый терминал в сети TCP/IP имеет адреса трех уровней:

- физический (MAC-адрес) — локальный адрес узла, определяемый технологией, с которой построена отдельная сеть, в которую входит данный узел. 11-AO-17-3D-BC-01
- сетевой (IP-адрес), состоящий из 4 байт, 109.26.17.100.
- символьный (DNS-имя) — идентификатор-имя, SERVI.IBM.COM

MAC-адрес – это локальный адрес узла, определяемый технологией, с которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в LAN - это MAC-адрес сетевого адаптера или порта маршрутизатора. MAC-адрес назначается производителями оборудования и является уникальным адресом. Для всех существующих технологий LAN MAC-адрес имеет формат 6 байтов (см.рис.5.6):

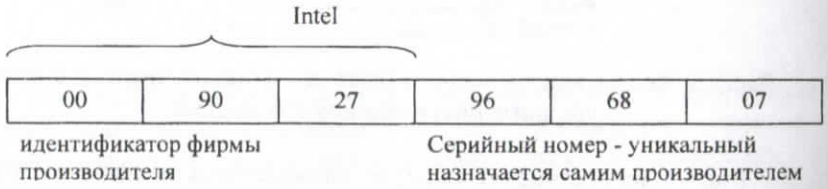



Рис.5.6. Структура MAC-адреса

IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов, состоит из двух частей: номера сети Net_id и номера узла host_id. Номер сети Net_id может быть выбран администратором произвольно или назначен по рекомендации NIC (Network Information Center), если сеть работает как составная часть Интернет. Обычно провайдеры услуг Интернет, получают диапазоны подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое. Узел может входить в несколько IP-сетей. В этом случае, узел должен иметь несколько IP-адресов, по числу сетевых связей. IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.



DNS-имя (символьный адрес) назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, пользуется на прикладном уровне (см. рис.5.7). Служба DNS (Domain Name System) рассматривается далее в разделе 5.6.

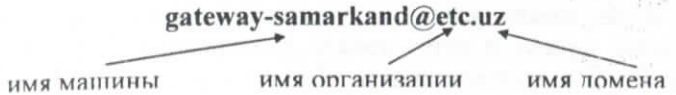



Рис.5.7. Структура DNS-имени

Рассмотрим основные классы IP-адресов. Напомним, IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:

128.10.2.30 - традиционная десятичная форма представления адреса,

10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса. На рис.5.8 показана структура IP-адреса.

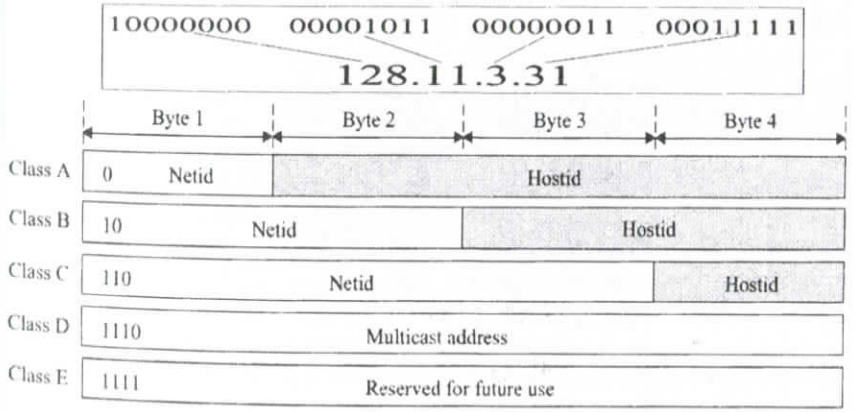



Рис.5.8. Структура IP-адреса

Адрес состоит из двух логических частей — номера сети и номера узла в сети. Каких часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей) В сетях класса A количеств узлов должно быть больше $2^{16}$, но не превышать $2^{24}$.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов $2^8$-$2^{16}$. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше $2^8$. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес — multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

На рис.5.9 приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

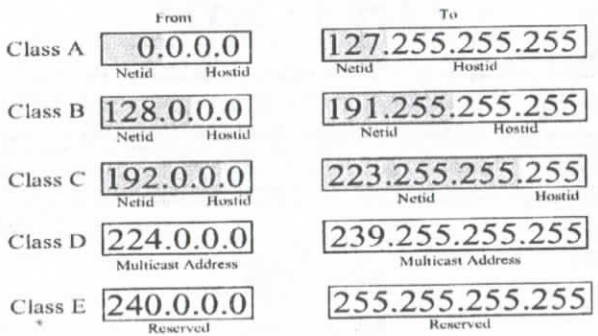



Рис.5.9. Диапазоны номеров сетей



Рассмотрим отображение физических адресов на IP-адреса. Локальный адрес используется в протоколе IP только в пределах LAN при обмене данными между маршрутизатором и узлом этой сети. Маршрутизатор, получив пакет узла одной из сетей, непосредственно подключенных к его портам, должен для передачи пакета сформировать кадр в соответствии с требованиями принятой в этой сети технологии и указать в нем локальный адрес узла (например его MAC-адрес). В пришедшем пакете этот адрес не указан, поэтому перед маршрутизатором встает задача поиска его по известному IP-адресу, который указан в пакете в качестве адреса назначения.

С аналогичной задачей сталкивается конечный узел, когда он хочет отправить пакет в удаленную сеть через маршрутизатор, подключенный к той же локальной сети, что и данный узел.

Протокол ARP Address Resolution Protocol служит для определения локального адреса по IP-адресу. Протокол ARP работает различным образом в зависимости от протокола канального уровня, работающего в данной сети:

– Ethernet, Token Ring, FDDI - протоколы с возможностью широковещательного доступа одновременно ко всем узлам сети,
– X.25, Frame Relay - протоколы глобальной сети, не поддерживающий широковещательный доступ.

Протокол ARP реализует следующий алгоритм:

1. В локальных сетях протокол ARP использует широковещательные кадры протокола уровня для поиска в сети узла с заданным IP-адресом.
2. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.
3. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным.
4. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес.
5. ARP-запросы и ответы используют один и тот же формат пакета.

Формат пакета протокола ARP зависит от типа сети, т.к. локальные адреса могут иметь различную длину в различных типах сетей. В глобальных сетях администратору сети чаще всего приходится

вручную формировать ARP-таблицы, в которых он задает, соответствие IP-адреса адресу узла сети X.25

Для автоматизации процесса назначения IP-адресов используется протокол DHCP – протокол динамической настройки хоста Dynamic Host Configuration Protocol. Протокол DHCP использует модель клиент-сервер. При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, это дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов. DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением.

Протокол DHCP имеет следующие недостатки:

- проблема согласования информационной адресной базы в службах DHCP и DNS;
- нестабильность IP-адресов усложняет процесс управления сетью. Системы управления, основанные на протоколе SNMP, разработаны с расчетом на статичность IP-адресов
- централизация процедуры назначения адресов снижает надежность системы
- при отказе DHCP-сервера все его клиенты оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации - использование в сети нескольких серверов DHCP, со своими пулами IP-адресов.

Протокол LDAP (Lightweight Directory Access Protocol – упрощенный протокол доступа к каталогам) является стандартом доступа к службам сетевых каталогов, а протокол DHCP используется для динамического присвоения IP-адресов пользователям для доступа к сетевым ресурсам.

Протокол LDAP упрощает работу в сетевой среде. Пользователи получают возможность входить в систему с любого узла сети и работать с привычными для себя настройками, поскольку информация о них будет сохраняться в основанном на LDAP каталоге. В будущем основанные на LDAP каталоги могут применяться для поддержки инфраструктуры интрасетей и Internet. Например, службы DNS и DHCP будут использовать серверы



каталогов на базе LDAP в качестве своих хранилищ информации. Тогда эти службы приобретут дополнительные достоинства — модульную структуру и независимость от места размещения.

Протокол LDAP специально предназначен для использования с управляющими и браузерными приложениями, которые обеспечивают интерактивный доступ к каталогам с возможностью чтения и записи. LDAP – это протокол взаимодействия клиента и сервера, обеспечивающий доступ к службе каталогов и работающий непосредственно поверх протокола TCP/IP.

Применяемая в LDAP информационная модель основана на схеме, использованной в протоколе X.500, которая базируется на «именных записях». Именные записи обозначают реальные объекты (например, какого-нибудь пользователя) или некоторую сетевую службу (например, службу преобразования адресов). Каждая запись сопровождается атрибутами, имеющими одно или несколько значений, и хранит информацию, которую при необходимости можно найти. Как правило, каталог на базе LDAP поддерживает репликацию, что повышает надежность и увеличивает быстродействие системы.

Главная цель объединения серверов - дать пользователям возможность встраивать их системы управления сетевыми адресами средства повышения надежности, безопасности и синхронизации имен и адресов.

Процесс взаимодействия серверов LDAP и DHCP показан на рис.5.10. Клиент запрос на доступ в Интернет с указанием нужного адреса и ресурса. Сервер DHCP автоматически присваивает клиенту IP-адрес и связывает пользователя с ресурсами в каталоге LDAF. Сервер LDAP находит указанные ресурсы и автоматически соединяет пользователя с узлом сети.


Рис.5.10. Процесс взаимодействия DHCP и LDAP

Как и DNS, LDAP — это служба каталогов в архитектуре клиент-сервер. Каталоги могут содержать самую разную информацию, например, БД пересчета телефонный номеров E.164 в IP-адреса для пользователей IP-телефонии.

### 5.5.1. Адресация в IPv6

Одним из основных отличий внедряемого в настоящее время протокола IPv6 от протокола IPv4 является использование более длинных адресов. Адреса получателя и источника в IPv6 имеют длину 128 бит или 16 байт.

В IPv6 принята новая форма записи адреса, т.к. при определении адреса сети граница маски часто не совпадает с границей байтов адреса, и десятичная запись в данном случае неудобна. Адрес записывается в шестнадцатиричном виде, каждые четыре цифры отделяются друг от друга двоеточием, например:

FEDC : OA96 : 0 : 0 : 0 : 0 : 7733 :567A.

Для сетей, поддерживающих обе версии протокола - IPv4 и IPv6 - имеется возможность использовать для младших 4 байтов традиционную десятичную запись, а для старших - шестнадцатиричную:

0 : 0 : 0 : 0 : 0 : FFFR 194.135.75.104

Версия 6 обобщает специальные типы адресов версии 4 в следующих типах адресов:

- Unicast — индивидуальный адрес. Определяет отдельный узел — компьютер или порт маршрутизатора. Пакет должен быть доставлен узлу по кратчайшему маршруту.
- Cluster — адрес кластера. Обозначает группу узлов, которые имеют общий адресный префикс (например, присоединенных к одной физической сети). Пакет должен быть маршрутизирован группе узлов по кратчайшему пути, а затем доставлен только одному из членов группы (например, ближайшему узлу).
- Multicast — адрес набора узлов, возможно в различных физических сетях. Копии пакета должны доставлены каждому узлу набора, используя аппаратные возможности групповой или широковещательной доставки, если это возможно.



Как и в версии IPv4, адреса в версии IPv6 делятся на классы, в зависимости от значения нескольких старших бит адреса.

Большая часть классов зарезервирована для будущего применения. Наиболее интересным для практического использования является класс, предназначенный для провайдеров услуг Internet, названный Provider-Assigned Unicast. Адрес этого класса имеет следующую структуру (рис.5.11):

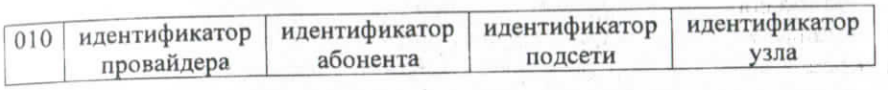



Рис.5.11. Структура адреса в IPv6

Каждому провайдеру услуг Интернет назначается уникальный идентификатор, которым помечаются все поддерживаемые им сети. Далее провайдер назначает своим абонентам уникальные идентификаторы и использует оба идентификатора при назначении блока адресов абонента. Абонент сам назначает уникальные идентификаторы своим подсетям и узлам этих сетей.

Абонент может использовать технику подсетей, применяемую в версии IPv4, для дальнейшего деления поля идентификатора подсети на более мелкие поля. Описанная схема приближает схему адресации IPv6 к схемам, используемым в территориальных сетях, включая телефонные сети или сети X.25. Иерархия адресных полей позволит магистральным маршрутизаторам работать только со старшими частями адреса, оставляя обработку менее значимых полей маршрутизаторам абонентов.

Под поле идентификатора узла требуется выделения не менее 6 байт, для того чтобы можно было использовать в IP-адресах MAC-адрес локальных сетей непосредственно.

Для обеспечения совместимости со схемой адресации версии IPv4, в версии IPv6 имеется класс адресов, имеющих 0000 0000 в старших битах адреса. Младшие 4 байта адрес этого класса должны содержать адрес IPv4. Маршрутизаторы, поддерживающие обе версии адресов, должны обеспечивать трансляцию при передаче пакета из сети, поддерживающий адресацию IPv4, в сеть, поддерживающую адресацию IPv6, и наоборот.

## 5.6. DNS – система доменных имен, принципы их распределения и распознавания

### 5.6.1. Служба трансляции имен Интернета – функции DNS

Интернет-хосты также имеют множество идентификаторов. Одним из идентификаторов является *имя хоста.* Имя хоста представляет собой мнемоничную, а следовательно, удобную для восприятия человеком запись, например cnn.com, www.yahoo.com,gaia.cs.umass.edu, surf.eurecom.fr. Недостатком имен хостов является то, что они не содержат информации о конкретном расположении хоста; единственным указателем на географическое местоположение может служить код страны (например, код fгуказывает на принадлежность хоста к Франции, и т. п.). Другой недостаток имен хостов заключается в их значительной длине, приводящей к существенным затратам на обработку маршрутизаторами. По указанным причинам был введен другой идентификатор хостов —*IP-адрес.* IP-адрес представляет собой совокупность четырех однобайтовых чисел и имеет жесткую иерархическую структуру. IP-адреса обычно записываются в виде четырех десятичных чисел, разделенных точками и представляющих значения каждого из байтов: 121.7.106.83. Каждое число находится в диапазоне от 0 до 255. Иерархичность IP-адресов заключается в том, что при их чтении слева направо мы получаем все более точную информацию о местонахождении хоста в Интернете (говоря точнее, мы определяем принадлежность хоста к той или иной сети, входящей в сеть сетей — Интернет).

Как мы видели, существуют два принципиально разных способа идентификации хостов: с помощью имен и с помощью IP-адресов. Имя хоста удобно для людей в силу своей мнемоничности, а IP-адрес, являющийся компактной числовой величиной фиксированного размера, проще обрабатывать маршрутизаторами. Для того чтобы установить связь между этими двумя идентификаторами, используется *система доменных имен* (Domain Name System, DNS). DNS представляет собой с одной стороны, базу данных, распределенную между иерархически структурированными *серверами имен*, и, с другой стороны, протокол прикладного уровня, организующий взаимодействие между хостами и серверами имен для выполнения операций преобразования. Протоколу DNS назначен



порт с номером 53, и работает DNSповерх протокола UDPтранспортного уровня.

Обычно DNS используется другими протоколами прикладного уровня: HTTP, SMTPи FTPдля получения IP-адресов вместо вводимых пользователями имен хостов. Рассмотрим, к примеру, ситуацию, когда пользователь вводит в адресной строке браузера адрес web-страницы www.someschool.edu/index.html. Для того чтобы сформировать запрос, пользовательский хост должен сначала получить IP-адрес удаленного хоста, на котором находится ресурс, то есть www.someschool.edu. При работе протокола DNS пользовательский хост играет роль клиента. Браузер выделяет из URL-адреса страницы имя хоста и передает его клиентской стороне DNS- приложения, которая формирует и отправляет запрос DNS-серверу. DNS-сервер обрабатывает запрос и отсылает клиенту ответ, содержащий IP-адрес хоста. Затем браузер открывает TCP-соединение с HTTP-сервером, выполняющимся на хосте с полученным IP-адресом. Очевидно, что процесс получения IP-адреса не является мгновенным и вносит дополнительную задержку в суммарное время установления соединения с HTTP-сервером, которая иногда может быть весьма значительной.

Помимо преобразования имен хостов в IP-адреса, DNS выполняет еще несколько важных функций, перечисленных ниже.

- *Поддержка псевдонимов серверов.* Хосты с длинными именами могут иметь один или несколько псевдонимов; например, хосту relayl.west-coast.enterprise.com можно присвоить два псевдонима — enterprise.com и www.enterprise.com. В этом случае говорят, что relayl.west-coast.enterprise.com является каноническим именем хоста. Обычно введение псевдонимов вызывается недостаточной мнемоничностью канонического имени. Получение канонического имени хоста по заданному псевдониму, как и IP-адреса, выполняется с помощью протокола DNS.
- *Поддержка псевдонимов почтовых серверов.* Очевидно, что мнемоничность особенно важна для адресов электронных почтовых ящиков. Например, если Боб использует почтовый ящик компании Hotmail, то его адрес будет иметь вид bob@hotmail.com, что нетрудно запомнить. На самом деле hotmail.com является лишь псевдонимом почтового сервера Боба, в то время как каноническое имя имеет гораздо более сложную структуру, например relayl.west-coast.hotmail.com.

### 5.6.2. Общие принципы функционирования DNS

Ниже мы опишем основную схему функционирования DNS. Основным предметом рассмотрения для нас будет являться преобразование имени хоста в соответствующий IP-адрес.

Предположим, что некоторому приложению (web-браузеру или программе чтения электронной почты), выполняющемуся на хосте пользователя, необходимо получить IP-адрес удаленного хоста. Приложение вызывает клиентскую сторону DNS и передает ей имя нужного хоста. Клиентская сторона, в свою очередь, создает запрос, отсылает его DNS-серверу и ждет ответа. Как правило, время ответа DNS-сервера составляет от нескольких миллисекунд до десятков секунд. Ответ представляет собой сообщение, содержащее группу из одного или нескольких IP-адресов, которые передаются DNS-клиентом вызвавшему его приложению.

DNS является замечательным примером того, как в Интернете может быть организована распределенная база данных (см.рис.5.12)[51].

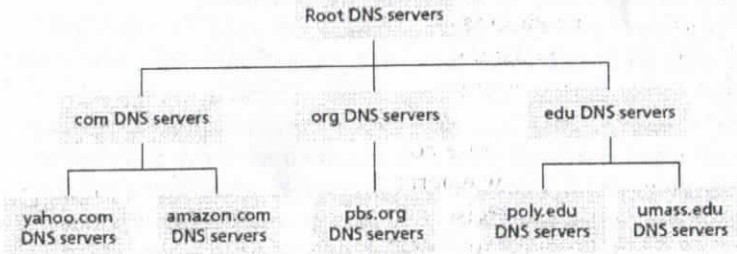



Рис.5.12. Иерархическая структура серверов DNS

Для того чтобы решить проблему хранения больших объемов информации, система DNS была спроектирована в виде совокупности многочисленных серверов имен, рассредоточенных по всему миру и организованных в виде иерархической структуры. Ни один сервер имен не содержит информации обо всех IP-адресах хостов; эта информация распределена между множеством серверов.

[51] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



Можно ввести следующую укрупненную классификацию серверов имен: локальные, корневые и полномочные.

- *Корневые серверы имен.* Число корневых серверов имен в Интернете равно 13, и большинство из них находится в Северной Америке. Рис.5.13 иллюстрирует положение корневых серверов имен на географической карте мира в октябре 2006г[52].

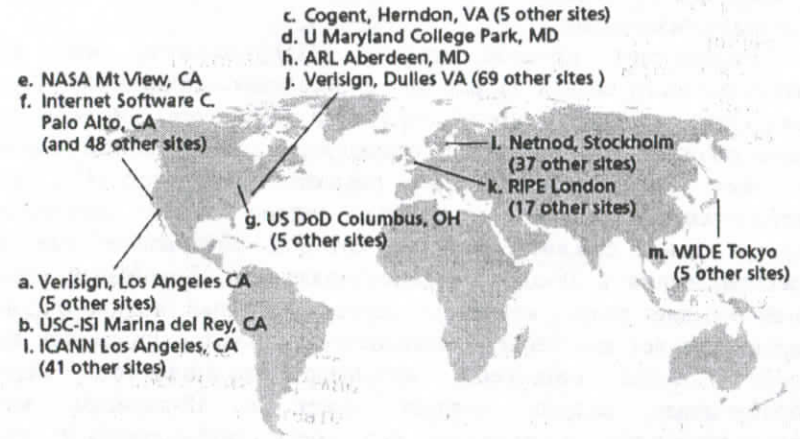



Рис.5.13. Корневые серверы DNS в конце 2006г. (имя, организация, расположение)

- *Сервера доменов верхнего уровня* (Top-level domain TLD servers). Эти сервера отвечают за домены верхнего уровня, такие как com, org, net, edu и gov, а также за национальные домены, такие как uk, fr, ca и jp.
- *Полномочный сервер имен* — это сервер, на котором зарегистрирован данный хост. Обычно хосты регистрируются на локальных серверах имен Интернет-провай- деров (на самом деле в целях обеспечения надежности хосты регистрируются не менее чем на двух полномочных серверах). Полномочный сервер содержит информацию о связи имени хоста с его IP-адресом.
- *Локальные серверы имен* имеются у каждого Интернет-провайдера (локальные серверы имен также называют серверами имен по умолчанию). Когда пользовательский хост посылает DNS-запрос,

[52] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

этот запрос сначала попадает на локальный сервер имен. Обычно локальный сервер имен расположен на относительно небольшом расстоянии от пользовательского хоста. В случае, если Интернет-провайдером является государственное или коммерческое учреждение, сервер имен принадлежит локальной сети организации; для резидентных Интернет-провайде- ров сервер имен обычно отделен от пользователя не более чем несколькими маршрутизаторами.

Рассмотрим простой пример. Предположим, что хост **surf.eurecom.fr** создал запрос IP- адреса **gaia.cs.umass.edu.** Пусть локальный сервер имен института Eurecom имеет имя **dns.eurecom.fr,** а полномочный сервер имен хоста **gaia.cs.umass.edu** — имя **dns.umass.edu.** Как показано на рис.5.14[53], хост **surf.eurecom.fr** сначала отправляет запрос своему локальному серверу имен **dns.eurecom.fr,** в котором содержится имя для преобразования в IP-адрес **(gaia.cs.umass.edu).** Локальный сервер имен передает запрос корневому серверу, который, в свою очередь, перенаправляет его серверу, являющемуся полномочным для всех хостов домена **umass.edu,** например **dns.umass.edu.** Сервер обрабатывает запрос, создает ответ с IP-адресом хоста **gaia.cs.umass.edu** и отсылает его хосту **surf.eurecom.fr** через корневой и локальный серверы имен. Обратите внимание на то, что в этом примере процедура получения IP-адреса требует передачи шести DNS-сообщений: трех запросов и трех ответов.

Выше было сделано допущение о том, что корневой сервер имен располагает IP- адресами полномочных серверов для любого хоста. На самом деле это допущение неверно. Корневой сервер «знает» адрес лишь промежуточного сервера имен, который содержит IP-адрес полномочного сервера хоста.

Все приведенные выше примеры строились на основе допущения о том, что все DNS-запросы являются *рекурсивными.* Это означает, что, когда хост или сервер имен А обращается к серверу имен В, последний предпринимает необходимые для получения требуемого IP-адреса действия от имени А и передает его А. Протокол DNS предусматривает также *итеративные* запросы. Итеративные запросы отличаются от рекурсивных тем, что в случае

[53] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



отсутствия искомого IP-адреса сервер имен В возвращает А IP-адрес следующего сервера имен в цепочке, к которому А должен обратиться самостоятельно.

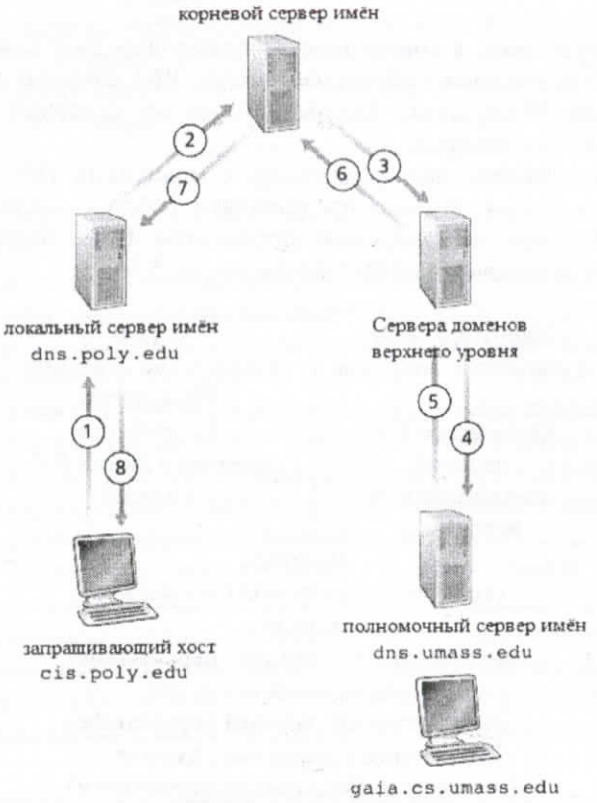



Рис.5.14. Рекурсивные запросы при получении IP-адреса gaia.cs.umass.ed

Последовательность запросов, необходимых для получения IP-адреса хоста, может содержать одновременно и рекурсивные, и итеративные запросы. На практике часто встречаются ситуации, когда все запросы являются рекурсивными за исключением единственного итеративного запроса локального сервера имен к корневому. Это объясняется тем, что корневые серверы вынуждены

обрабатывать значительное число запросов, а итеративный механизм снижает трудоемкость обработки запроса сервером.

### 5.6.3. DNS-записи и DNS-сообщения

Серверы имен, в совокупности образующие базу данных DNS, хранят *ресурсные записи* (Resource Records, RR), связывающие имена хостов с их IP-адресами. Каждый DNS-ответ содержит одну или более ресурсных записей.

В этом разделе мы столкнулись с понятиями DNS-запроса и DNS-ответа. Запрос и ответ представляют собой единственные два типа сообщений, используемые протоколом DNS. Форматы этих сообщений совпадают и представлены на рис.5.15.

| Идентификатор | Флаги |
|---|---|
| Количество вопросов | Количество ответных RR-записей |
| Количество RR-записей полномочного источника | Количество дополнительных RR-записей |
| Вопросы (количество вопросов переменное) | |
| Ответы (количество RR-записей переменное) | |
| Полномочный источник (количество RR-записей переменное) | |
| Дополнительная информация (количество RR-записей переменное) | |

Рис.5.15. Формат DNS-сообщения

Ниже приведено описание структуры:

- Первые 12 байт составляют *заголовочную секцию*, состоящую из нескольких полей. Первое поле представляет собой 16-разрядное число, идентифицирующее запрос. Идентификатор запроса копируется в ответное сообщение, что позволяет клиенту сопоставлять ответы с запросами. Поле флагов включает



одноразрядный флаг «запрос/ответ» и определяет, является ли сообщение запросом (0) или ответом (1). Одноразрядный флаг полномочности устанавливается для ответного сообщения в случае, если сервер имен является полномочным для запрашиваемого имени. Одноразрядный флаг предпочтительности рекурсии устанавливается в случае, когда клиенту (хосту или серверу имен) необходимо дать указание серверу имен применить рекурсивный запрос при отсутствии IP-адреса. Одноразрядный флаг доступности рекурсии устанавливается в ответном сообщении, если сервер имен поддерживает рекурсивный механизм запросов. В заголовке также содержатся четыре секции для «типов» данных.

- *Секция вопросов* содержит информацию о запросе и включает поле имени, в котором указано имя запрашиваемого хоста, и поле типа, определяющее содержание ответа, например адрес хоста (тип A) или имя почтового сервера.
- *Секция ответов* присутствует в ответных сообщениях и содержит требуемые ресурсные записи. Поскольку имени хоста может быть сопоставлено несколько IP-адресов (например, из-за дублирования web-серверов, упоминавшегося в этой главе), секция ответов также может содержать несколько записей.
- *Секция полномочности* включает в себя записи о других полномочных серверах.
- *Дополнительная секция* содержит прочие «полезные» записи. Например, в поле ответов может находиться запись, хранящая каноническое имя почтового сервера, а в дополнительную секцию помещена запись типа A с IP-адресом почтового сервера.

### Контрольные вопросы

1. На каком уровне используются протоколы TCP/IP?
2. Каково назначение IP- протокола?
3. Каково назначение протокола TCP?
4. Каково назначение протоколов FTP, SNMP, Telnet, SMTP?
5. Что показывает физический адрес? сетевой адрес?
6. Какие протоколы входят в состав прикладного уровня?
7. Какие устройства принадлежат прикладному уровню?
8. Какие протоколы входят в состав транспортного уровня?
9. Какие устройства принадлежат транспортному уровню?

10. Какие протоколы входят в состав сетевого уровня?
11. Какие устройства принадлежат сетевому уровню?
12. Какие протоколы входят в состав уровня сетевого интерфейса?
13. Какие устройства принадлежат уровню сетевого интерфейса?
14. Дайте определение IP- адреса.
15. Перечислите виды IP-адресов.
16. Сколько классов сети определены на сегодняшний день?
17. Каким образом определяется какая часть IP адреса относится к номеру сети, а какая к номеру узла?
18. Для чего предназначен протокол ARP?
19. Что такое служба DNS?
20. Для чего предназначен протокол DHCP?



# 6. ПРОТОКОЛЫ СЕТЕВОГО УРОВНЯ TCP/IP

## 6.1. Функции сетевого уровня

В этом разделе мы рассмотрим, как сетевой уровень реализует службы связи между хостами. Мы увидим, что, в отличие от транспортного уровня, «кусок» сетевого уровня присутствует **в каждом хосте и маршрутизаторе сети**. Благодаря этому протоколы сетевого уровня являются одними из самых сложных (и поэтому одними из самых интересных).

На рис.6.1 изображена схема простой сети с двумя хостами, H1 и H2, и несколькими маршрутизаторами на пути от хоста H1 до хоста H2[54].

Пусть хост H1 посылает информацию хосту H2. Рассмотрим роль сетевого уровня на этих хостах и промежуточных маршрутизаторах. Сетевой уровень хоста H1 принимает сегменты от транспортного уровня хоста H1, инкапсулирует каждый сегмент в дейтаграмму (единицу обмена сетевого уровня), после чего отправляет дейтаграммы в путь к их адресату; то есть он посылает дейтаграммы своему ближайшему маршрутизатору R1. На принимающем хосте H2 сетевой уровень получает дейтаграммы от своего ближайшего маршрутизатора (в данном случае R2), извлекает сегменты транспортного уровня и доставляет их транспортному уровню хоста H2. Основная задача маршрутизаторов заключается в «продвижении» дейтаграмм из входных линий связи в выходные линии. Обратите внимание, что на рис.6.1 маршрутизаторы показаны с сокращенным стеком протоколов, то есть без уровней выше сетевого, потому что на маршрутизаторах не работают протоколы прикладного и транспортного уровней (исключая задачи контроля).

Таким образом, роль сетевого уровня обманчиво проста — перемещение пакетов от передающего хоста к принимающему. Для этого можно выделить две важные функции сетевого уровня.

- *Продвижение данных.* Когда пакет прибывает на вход маршрутизатора, маршрутизатор должен переместить его на соответствующую выходную линию.

[54] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

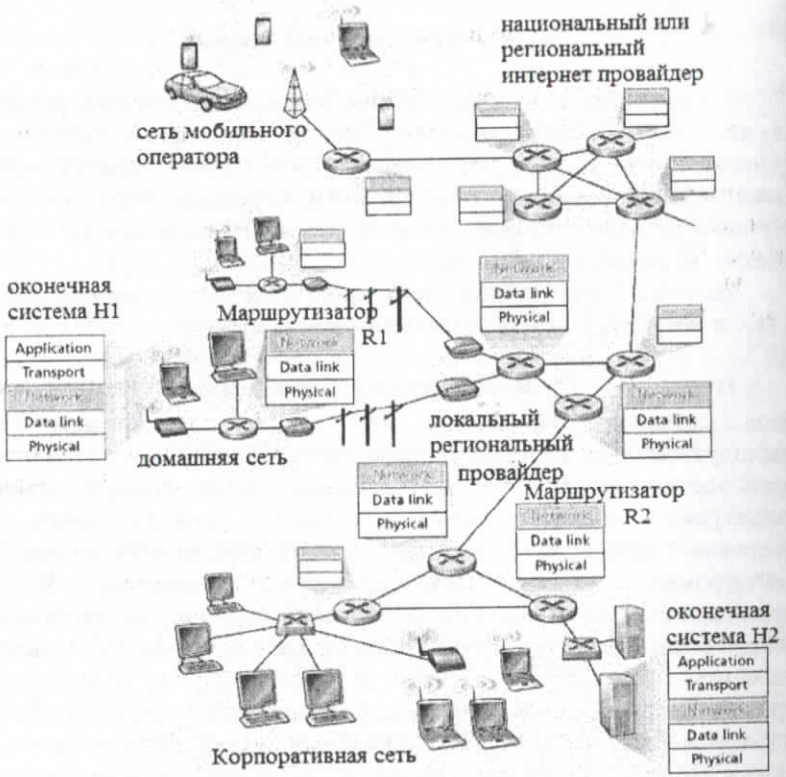



Рис.6.1. Сетевой уровень

Например, пакет, прибывающий с хоста H1 на маршрутизатор R2, должен быть передан следующему маршрутизатору на пути к хосту H2.

- *Определение пути.* Сетевой уровень должен определить маршрут, или путь, по которому следуют пакеты от отправителя к получателю. Алгоритмы, рассчитывающие эти маршруты, называются *алгоритмами маршрутизации.* Алгоритм маршрутизации определяет, например, путь, по которому пакеты движутся от хоста H1 к хосту H2.

Термины «маршрутизация» и «продвижение данных» многие



авторы часто путают и используют как синонимы. Мы постараемся применять эту терминологию более точно. «Маршрутизацией» мы будем называть глобальный (охватывающий всю сеть) процесс определения всего пути, который проходит дейтаграмма от отправителя до получателя. «Продвижением данных» мы станем называть локальные действия конкретного маршрутизатора по перемещению дейтаграммы из интерфейса входной линии связи в интерфейс выходной линии.

## 6.2. Интернет-протокол IP – основной протокол сетевого уровня

Сетевой уровень Интернета часто называют IP-уровнем (по названию протокола IP). Однако, сам протокол IP представляет собой лишь часть (хотя и очень важную) сетевого уровня Интернета. Как показано на рис.6.2, сетевой уровень Интернета состоит из трех основных компонентов[55].

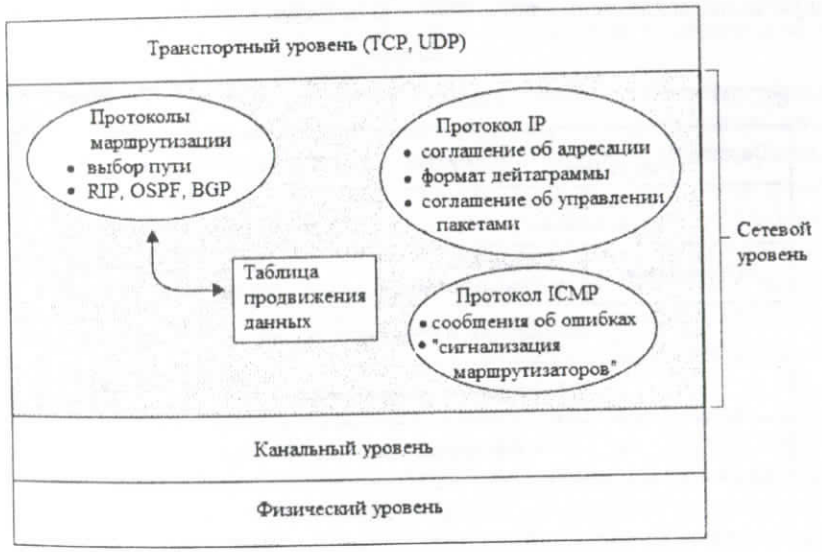



Рис.6.2. Состав сетевого уровня Интернета

[55] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

- Первый компонент представляет собой протокол сетевого уровня. Сетевой протокол в Интернете называется Интернет-протоколом, а чаще *протоколом IP* (Internet Protocol). Сегодня используются две версии протокола IP. В этой лекции мы обсудим широко распространенную версию 4, обычно называемую IPv4 (RFC 791). Протокол IPv6 (версия 6 RFC 2373, RFC 2460) должен в будущем заменить IPv4.
- Второй главной составляющей сетевого уровня является компонент определения пути. Он выбирает маршрут, по которому следует дейтаграмма от отправителя к получателю.
- Третий компонент сетевого уровня должен уметь сообщать об ошибках в дейтаграммах и отвечать на запросы определенной информации сетевого уровня. Эту задачу в Интернете решает протокол ICMP (Internet Control Message Protocol — протокол управляющих сообщений Интернета).

Формат дейтаграммы протокола IPv4 показан на рис.6.3. Ниже перечислены ключевые поля IPv4-дейтаграммы.

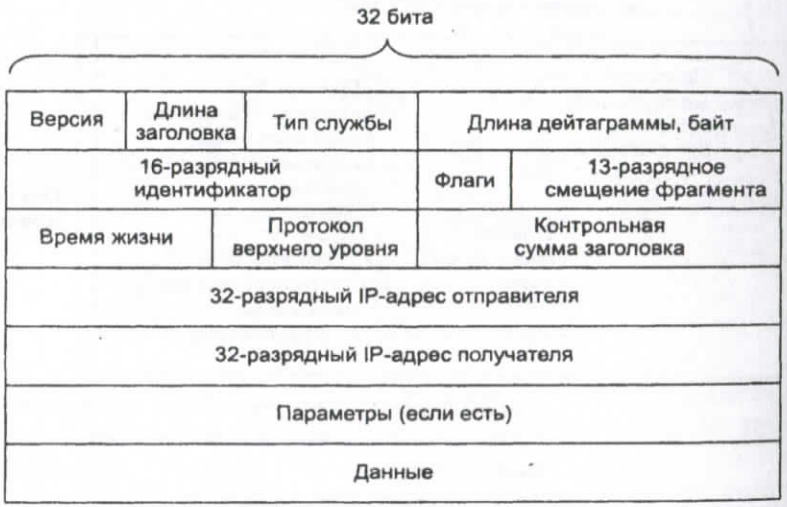



Рис.6.3. Формат IPv4- дейтаграммы

*Версия.* Четыре бита в этом поле определяют номер версии протокола IP. По этому номеру маршрутизатор может определить,



как интерпретировать остальные поля IP-дейтаграммы. В различных версиях протокола IP применяются различные форматы IP-дейтаграмм. На рисунке показан формат дейтаграммы текущей версии протокола IP (IPv4).

*Длина заголовка.* Поскольку IPv4-дейтаграмма может содержать разное количество необязательных полей параметров (включаемых в заголовок IPv4-дейтаграммы), эти четыре бита необходимы для того, чтобы определить, где заканчивается заголовок и начинаются данные. В большинстве IP-дейтаграмм не содержатся поля параметров, поэтому обычно заголовок IP-дейтаграммы 20-разрядный.

*Тип службы.* Поле типа службы (Type Of Service, TOS) было включено в заголовок IPv4-дейтаграммы, чтобы была возможность разделять IP-дейтаграммы на типы (например, выделять дейтаграммы, для которых требуется низкая задержка, или высокая пропускная способность, или высокая надежность). Так, может оказаться полезным отличать дейтаграммы реального времени (например, используемые в IP-телефонии) от прочего трафика (например, FTP). Предоставляемый уровень услуг определяется администратором маршрутизатора.

*Длина дейтаграммы.* Это полная длина IP-дейтаграммы (заголовок плюс данные) в байтах. Поскольку размер этого поля равен 16 бит, теоретически максимальный размер IP-дейтаграммы может составлять 65 535 байт. Однако размер дейтаграмм редко превосходит 1500 байт и обычно ограничивается значением 576 байт.

*Идентификатору флаги, смещение фрагмента.* Эти три поля имеют отношение к так называемой IP-фрагментации. Этот вопрос мы подробно рассмотрим чуть позже. Интересно отметить, что новая версия протокола IP (IPv6) запрещает фрагментацию в маршрутизаторах.

*Время жизни.* Поле времени жизни (Time To Live, TTL) позволяет гарантировать, что дейтаграммы не будут вечно циркулировать в сети (например, из-за существующей в течение долгого времени маршрутной петли). Значение этого поля уменьшается на единицу на каждом маршрутизаторе. Когда значение поля TTL достигает нуля, маршрутизатор отбрасывает дейтаграмму.

*Протокол.* Это поле используется только тогда, когда IP-дейтаграмма достигает конечного адресата. Значение поля определяет протокол транспортного уровня, которому следует передать данные из IP-дейтаграммы. Например, значение 6 означает,

Проблема заключается в том, что в каждой линии связи на пути от отправителя до получателя могут использоваться разные протоколы канального уровня, и у каждого из этих протоколов может быть свой, отличный от других, максимальный размер поля данных.

Чтобы лучше разобраться в этой проблеме, представьте себе маршрутизатор, соединяющий несколько линий, в каждой из которых применяется свой, отличный от других протокол канального уровня со своим максимальным размером поля данных. Предположим, маршрутизатор получает IP-дейтаграмму по одной линии и заглядывает в свою таблицу продвижения данных, чтобы определить исходящую линию для этой дейтаграммы. Предположим также, что максимальный размер поля данных в исходящей линии меньше длины IP-дейтаграммы. Впору запаниковать, поскольку нужно сжимать слишком большой IP-пакет так, чтобы он поместился в поле полезной нагрузки пакета канального уровня. Решение этой проблемы состоит в разбиении содержащихся в IP-дейтаграмме данных на несколько IP-дейтаграмм меньшего размера. Каждую из этих IP-дейтаграмм меньшего размера называют *фрагментом.*

Прежде чем фрагменты достигнут транспортного уровня адресата, из них необходимо снова собрать исходную дейтаграмму. Действительно, протоколы TCP и UDP ожидают получить от сетевого уровня полный, не фрагментированный пакет. Разработчики протокола IPv4 понимали, что повторная сборка (и, возможно, повторная фрагментация) дейтаграмм на маршрутизаторах значительно усложнит протокол и снизит производительность маршрутизаторов. (Если бы вы были маршрутизатором, захотели бы вы сверх всех ваших обязанностей заниматься еще и повторной сборкой фрагментированных дейтаграмм?) Придерживаясь принципа сохранения простоты сетевого уровня, разработчики IPv4 решили оставить задачу повторной сборки фрагментированных дейтаграмм оконечным системам.

Когда хост-адресат получает серию дейтаграмм, он должен определить, являются ли данные дейтаграммы фрагментами некой исходной дейтаграммы большего размера. Если он выясняет, что некие дейтаграммы представляют собой фрагменты, ему нужно также идентифицировать последний фрагмент дейтаграммы, чтобы можно было собрать эти фрагменты вместе в оригинальную дейтаграмму и выяснить, как это делается. Чтобы хост-получатель мог осуществлять повторную сборку дейтаграмм, разработчики IPv4 поместили в



дейтаграмму поля *идентификации*, *флага* и *фрагментации.* Когда дейтаграмма создается, хост-отправитель маркирует ее номером-идентификатором, а также помещает в нее адреса отправителя и получателя. Хост-отправитель увеличивает на единицу идентификационный номер для каждой следующей посылаемой дейтаграммы. Когда маршрутизатору необходимо фрагментировать дейтаграмму, каждый получающийся фрагмент помечается адресом отправителя, адресом получателя и идентификационным номером оригинальной дейтаграммы. Когда хост-адресат получает серию дейтаграмм от одного и того же передающего хоста, он изучает идентификационные номера дейтаграмм, чтобы определить, являются ли данные дейтаграммы фрагментами дейтаграммы большего размера. Поскольку протокол IP предоставляет ненадежную службу, один или несколько фрагментов могут не достичь адресата. Чтобы хост-адресат мог быть абсолютно уверен в том, что получил последний фрагмент оригинальной дейтаграммы, бит флага в последнем фрагменте устанавливается в 0, тогда как во всех остальных фрагментах он устанавливается в 1. Кроме того, чтобы хост-адресат мог определить, не был ли потерян какой-либо из фрагментов (а также иметь возможность собрать фрагменты оригинальной дейтаграммы в правильном порядке), в каждом фрагменте имеется поле смещения.

На рис.6.4 изображен пример[56]. Дейтаграмма из 4000 байт (20 байт IP-заголовка и 3980 байт полезной нагрузки) прибывает на маршрутизатор и должна быть переправлена далее по линии с максимальным размером поля данных в 1500 байт. Это означает, что 3980 байт оригинальной дейтаграммы должны быть распределены между тремя отдельными фрагментами (каждый из которых также представляет собой IP-дейтаграмму). Предположим, что оригинальная дейтаграмма маркирована идентификационным номером 777. Характеристики трех фрагментов показаны в табл.6.1. Полезная нагрузка дейтаграммы передается транспортному уровню получателя только после того, как IP-уровень полностью восстановит оригинальную дейтаграмму. Если один или несколько фрагментов не сумеют достичь адресата, вся дейтаграмма отбрасывается и не передается транспортному уровню.

[56] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

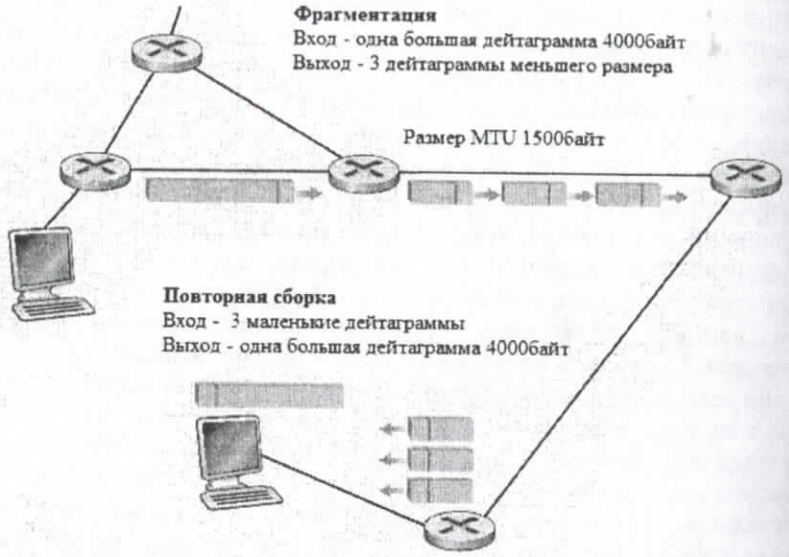



Рис.6.4. Фрагментация и повторная сборка IP-дейтаграммы

Таблица 6.1.

IP-фрагменты

| Фрагмент | Байты | ID | Смещение | Флаг |
|---|---|---|---|---|
| 1 | 1480 | 777 | 0 | 1 |
| 2 | 1480 | 777 | 1480 | 1 |
| 3 | 1020 = 3980- 1480- 1480 | 777 | 2960 | 0 |

Но, как было показано в предыдущей главе, если в качестве транспортного уровня используется протокол TCP, тогда восстановлением после потери фрагмента занимается протокол TCP, повторяя передачу всех данных оригинальной дейтаграммы.

Фрагментация и повторная сборка накладывают дополнительное бремя на Интернет-маршрутизаторы (фрагментация) и на хосты-адресаты (повторная сборка). Поэтому желательно свести фрагментацию к минимуму. Для этого часто ограничиваются размеры TCP- и UDP-сегментов, что снижает вероятность фрагментации.



## 6.3. Протокол определения адресов (ARP) и протокол определения сетевого адреса по местоположению (RARP)

На рис.6.5 приведён пример коммутируемой локальной сети, соединяющей 3 отдела, 2 сервера, посредством маршрутизатора и 4 коммутаторов (switch). Т.к. эти коммутаторы работают на канальном уровне, они коммутируют кадры канального уровня (аналогично дейтаграммам на сетевом уровне), не распознавая адресов сетевого уровня и не используя протоколы маршрутизации типа RIP или OSPF для определения маршрута через сеть между коммутаторами 2 уровня.

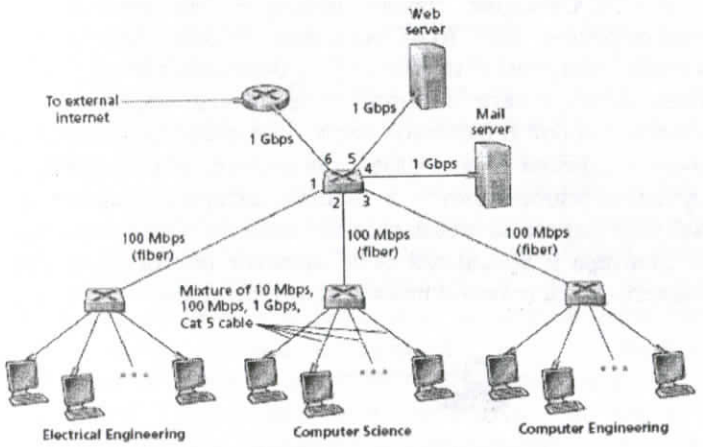



Рис.6.5. Коммутируемая локальная сеть, соединенная посредством 4 коммутаторов (switch)

Узлы локальной сети (LAN) посылают друг другу кадры по широковещательному каналу. Это означает, что кадр, переданный одним узлом локальной сети, принимается всеми остальными узлами этой локальной сети. Но, как правило, узлу локальной сети нужно передать кадр не *всем* узлам сети, а одному *определенному* узлу. Чтобы предоставить ему такую возможность, у узлов локальной сети должны быть адреса, и адрес получателя должен указываться в поле кадра канального уровня. В этом случае, получив кадр, узел может

определить, предназначается этот кадр ему или какому-то другому узлу локальной сети.

- Если адрес получателя в кадре совпадает с адресом получившего этот кадр узла, тогда узел извлекает из кадра канального уровня дейтаграмму сетевого уровня и передает ее вверх по стеку протоколов.
- Если адрес получателя в кадре не совпадает с адресом получившего этот кадр узла, тогда узел просто отбрасывает этот кадр.

В действительности адрес в локальной сети есть не у узла, а у сетевого адаптера. Это иллюстрирует рис.6.6. **Адрес в локальной сети**, или **LAN-адрес**, также называют **физическим адресом, Ethernet-адресом** или **MAC-адресом** (Media Access Control — управление доступом к носителю). В большинстве локальных сетей (включая Ethernet-сети и сети с передачей маркера) LAN-адрес представляет собой 6-байтовое число, что позволяет использовать $2^{48}$ возможных адресов. Как показано на рис.6.6, эти 6-байтовые адреса, как правило, изображаются в шестнадцатеричном виде, при этом каждый байт адреса записывается как пара шестнадцатеричных цифр. Адрес адаптера в локальной сети является постоянным. Этот адрес прошивается в постоянной памяти адаптера при его изготовлении.

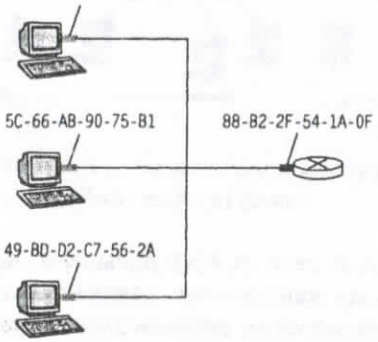



Рис.6.6. У каждого адаптера, соединенного с локальной сетью, есть уникальный адрес

Одно интересное свойство LAN-адресов заключается в том, что не может существовать двух адаптеров с одинаковыми адресами. Это может показаться удивительным, так как сетевые адаптеры



производятся в разных странах, разными производителями. Как может компания, производящая адаптеры в Тайване, гарантировать, что адреса ее адаптеров будут отличаться от адресов адаптеров, производимых другой компанией в Бельгии? Физическим адресным пространством управляет институт IEEE. Когда компания хочет выпускать адаптеры, она приобретает блок адресного пространства, состоящий из $2^{24}$ адресов. IEEE выделяет блок из $2^{24}$ адресов, фиксируя старшие 24 бита физического адреса и позволяя компании создавать уникальные комбинации из младших 24 разрядов для каждого адаптера.

Таким образом, LAN-адреса адаптеров образуют плоскую (в отличие от иерархической) структуру и не изменяются при перемещении адаптеров. У мобильного компьютера с Ethernet-картой всегда один и тот же LAN-адрес независимо от того, где находится этот компьютер. Вспомним, что IP-адреса, напротив, образуют иерархическую структуру (то есть делятся на сетевую и хостовую части), и при перемещении хоста IP-адрес узла должен быть изменен.

Когда адаптер хочет переслать кадр другому адаптеру в той же локальной сети, передающий адаптер помещает в кадр адрес получателя в локальной сети. Получив кадр, принимающий адаптер извлекает из него дейтаграмму и передает ее вверх по стеку протоколов. Все остальные адаптеры этой локальной сети также получают этот кадр, но они отбрасывают его, не передавая дейтаграммы сетевого уровня вверх по стеку протоколов. Однако иногда передающий узел бывает заинтересован в том, чтобы все адаптеры в локальной сети приняли и обработали кадр, который он посылает. В этом случае передающий адаптер помещает в поле адреса получателя специальный *широковещательный адрес*. В локальных сетях, использующих 6-байтовые адреса, широковещательный адрес представляет собой строку из 48 двоичных единиц (то есть FF-FF-FF-FF-FF-FF в шестнадцатеричной нотации).

Есть несколько причин, по которым узлам помимо адресов сетевого уровня выделяются LAN-адреса. Во-первых, локальные сети разрабатываются для работы с произвольными протоколами сетевого уровня, а не только с протоколом IP и Интернетом. Если бы вместо «нейтральных» LAN-адресов адаптерам назначались IP-адреса, адаптерам было бы трудно поддерживать другие протоколы сетевого уровня (например, IPX или DECnet). Во-вторых, если бы адаптеры

222.222.222.220 желает переслать дейтаграмму узлу 222.222.222.222. В этом случае передающий узел определяет нужный ему адрес при помощи протокола ARP. Сначала передающий узел формирует специальный *ARP-пакет*. В ARP-пакете содержится несколько полей, среди которых есть IP-адреса и LAN-адреса передающего и принимающего узлов. Для обоих ARP-пакетов (запроса и ответа) используется один и тот же формат. Цель ARP-пакета с запросом состоит в том, чтобы опросить все остальные узлы локальной сети и определить LAN-адрес, соответствующий интересующему нас IP-адресу.

Таблица 6.2.

Пример ARP-таблицы для узла с LAN-адресом 222.222.222.220

| IP-адрес | LAN-адрес | TTL |
|---|---|---|
| 222.222.222.221 | 88-B2-2F-54-1A-0F | 13:45:00 |
| 222.222.222.223 | 5C-66-AB-90-75-B1 | 13:52:00 |

Итак, в нашем примере узел 222.222.222.220 передает ARP-пакет с запросом своему адаптеру вместе с указанием переслать этот пакет по широковещательному LAN-адресу FF-FF-FF-FF-FF-FF. Адаптер помещает ARP-пакет в кадр канального уровня, указывает широковещательный адрес в поле адреса получателя и передает кадр в локальную сеть. Кадр с ARP-запросом принимается всеми остальными адаптерами локальной сети, и (поскольку в запросе использовался широковещательный адрес) каждый адаптер передает содержащийся в кадре ARP-пакет своему узлу. Каждый узел проверяет, совпадает ли его IP-адрес с указанным IP-адресом получателя в ARP-пакете. Узел, IP-адрес которого совпадает с указанным в пакете, посылает запрашивающему узлу ответный ARP-пакет с указанным в нем соответствующим LAN-адресом. После этого запрашивающий узел 222.222.222.220 может обновить свою ARP-таблицу и отправить IP-дейтаграмму.

Следует сделать два интересных замечания о протоколе ARP. Во-первых, ARP-запрос посылается в широковещательном кадре, а ответ передается в стандартном кадре. Во-вторых, в протоколе ARP реализован принцип самонастройки (plug-and-play), так как ARP-таблица узла формируется автоматически — она не должна настраиваться системным администратором. И если узел



отсоединяется от локальной сети, соответствующая ему запись по истечении времени жизни удаляется из таблицы.

### 6.3.2. Передача дейтаграммы узлу за пределы локальной сети

Теперь должно быть ясно, как работает протокол ARP, когда узел хочет послать дейтаграмму другому узлу *той же самой* локальной сети (то есть той же IP-сети). Но теперь мы рассмотрим более сложную ситуацию, в которой узел локальной сети хочет послать дейтаграмму сетевого уровня узлу, находящемуся *за пределами* локальной сети (то есть в другую IP-сеть). Обсудим этот вопрос на примере сети, состоящей из двух локальных сетей, соединенных маршрутизатором (рис.6.8).

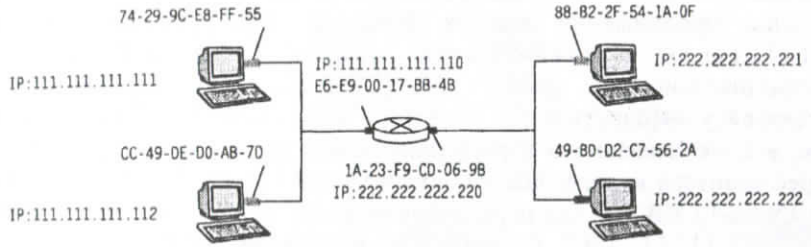



Рис.6.8. Две локальные сети, соединенные маршрутизатором

Обратите внимание, что существуют два типа узлов: хосты и маршрутизаторы. У каждого хоста есть ровно один IP-адрес и один адаптер. У маршрутизатора есть по одному IP-адресу для *каждого* интерфейса. У каждого интерфейса маршрутизатора есть собственный ARP-модуль и собственный адаптер. У изображенного на рисунке маршрутизатора два интерфейса, поэтому у него два IP-адреса, два ARP-модуля и два адаптера. Разумеется, у каждого адаптера есть свой LAN-адрес.

Адреса всех интерфейсов, соединенных с локальной сетью 1, имеют вид 111.111.111.xxx, а адреса всех интерфейсов, соединенных с локальной сетью 2, имеют вид 222.222.222.xxx. В данном примере первые три байта IP-адреса обозначают «сеть», а последний байт указывает на конкретный интерфейс в сети.

Теперь предположим, что хост 111.111.111.111 хочет переслать IP-дейтаграмму хосту 222.222.222.222. Передающий хост, как

обычно, отправляет дейтаграмму своему адаптеру. Но при этом передающий хост должен указать адаптеру LAN-адрес. Какой LAN-адрес следует использовать? Кое-кто может подумать, что это должен быть локальный адрес адаптера хоста 222.222.222.222, то есть 49-BD-D2-C7-56-2A. Однако это неверно. Если передающий адаптер будет использовать этот LAN-адрес, тогда ни один из адаптеров локальной сети 1 не станет передавать переданную IP-дейтаграмму своему сетевому уровню, так как адрес получателя в кадре не совпадет с LAN-адресом ни одного адаптера локальной сети 1. Переданная дейтаграмма просто умрет.

Если внимательно посмотреть на рис.6.8, то можно заметить, что для передачи дейтаграммы в локальную сеть 2 ее нужно направлять интерфейсу маршрутизатора по адресу 111.111.111.110. В таблице продвижения данных (таблице маршрутизации) хоста 111.111.111.111 должно быть указано, что дейтаграммы, предназначающиеся хосту 222.222.222.222, следует посылать интерфейсу маршрутизатора по адресу 111.111.111.110. Таким образом, в поле локального адреса получателя кадра следует указывать адрес адаптера интерфейса маршрутизатора 111.111.111.110, то есть E6-E9-00-17-BB-4B. Как передающему хосту узнать локальный адрес узла 111.111.111.110? С помощью протокола ARP. Как только передающий адаптер получает этот локальный адрес, он создает кадр и посылает его в локальную сеть 1. Адаптер маршрутизатора в локальной сети 1 видит, что данный кадр канального уровня адресован ему, и поэтому передает кадр сетевому уровню маршрутизатора. IP-дейтаграмма была успешно перемещена от хоста-отправителя на маршрутизатор! Но мы еще не закончили. Нам нужно еще переслать дейтаграмму от маршрутизатора получателю. Теперь маршрутизатор должен определить, по какому интерфейсу следует переслать дейтаграмму. Выбор делается при помощи таблицы маршрутизации, хранящейся на маршрутизаторе. В этой таблице маршрутизатор находит запись, по которой определяет, что дейтаграмму следует отправить через интерфейс 222.222.222.220. Этот интерфейс передает дейтаграмму своему адаптеру, который помещает дейтаграмму в новый кадр и посылает этот кадр в локальную сеть 2. Теперь уже LAN-адрес кадра указывает на его конечного получателя. И как же маршрутизатор узнает его LAN-адрес? При помощи протокола ARP, конечно!

Протокол ARP для Ethernet-сети определен в RFC 826.



## 6.4. Протокол управления сообщениями Интернета (ICMP)

Протокол IGMP (Internet Group Management Protocol — межсетевой протокол управления группами) версии 2, определенный в RFC 2236, работает между хостом и соединенным с ним напрямую маршрутизатором (этот маршрутизатор можно рассматривать как первый маршрутизатор на пути следования входящих дейтаграмм или последний маршрутизатор на пути следования исходящих дейтаграмм). На рис.6.9 изображены три групповых маршрутизатора, каждый из которых соединен с парой хостов через локальный интерфейс[57]. В данном примере локальный интерфейс связан с локальной сетью, и, как правило, несколько хостов локальной сети являются членами той или иной группы рассылки.

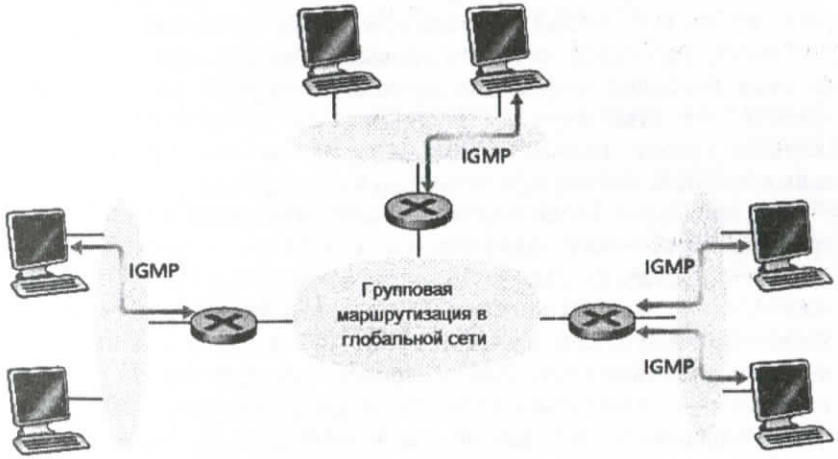



Рис.6.9. Две составляющие групповой рассылки сетевого уровня: протокол IGMP и протоколы групповой маршрутизации

Протокол IGMP предоставляет хосту средство информирования соединенного с ним маршрутизатора о том, что работающее на хосте приложение желает присоединиться к определенной группе

[57] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

рассылки. Учитывая ограниченность сферы действия протокола IGMP хостом и соединенным с ним маршрутизатором, для координирования групповых маршрутизаторов (включая присоединенные маршрутизаторы) в Интернете, очевидно, необходимы другие протоколы. Задачу координирования групповых маршрутизаторов решают *протоколы групповой маршрутизации сетевого уровня*, такие как PIM, DVMRP и MOSPF. Таким образом, групповая рассылка на сетевом уровне в Интернете состоит из двух взаимодополняющих компонентов: протокола IGMP и протоколов групповой маршрутизации.

Хотя протокол IGMP называют «протоколом членства в группах», этот термин может ввести в заблуждение, так как протокол IGMP действует локально, между хостом и соединенным с ним маршрутизатором. Несмотря на свое название, протокол IGMP не работает на всех хостах, входящих в группу рассылки. В действительности, протокола сетевого уровня, управляющего членством в группах рассылки и функционирующего на всех Интернет-хостах группы, *не существует.* Например, не существует протокола сетевого уровня, позволяющего хосту определить идентификаторы всех остальных хостов, присоединившихся к группе.

В протоколе IGMP версии 2 (RFC 2236) используются только три типа сообщений, приведенные в табл.6.3. Общее сообщение *membership_query* (запрос о членстве) посылается маршрутизатором всем хостам, присоединенным к его интерфейсу (например, всем хостам локальной сети), чтобы узнать обо всех группах рассылки, членами которых стали хосты данного интерфейса. С помощью специального сообщения *membership_query* маршрутизатор может также определить, вступил ли какой-либо хост, присоединенный к одному из его интерфейсов, в определенную группу рассылки. Этот специальный запрос включает адрес группы, помещаемый в специально отведенное для него поле.

Хосты отвечают на сообщение *membership_query* IGMP-сообщением *membership jreport.* Хост может также генерировать сообщения *membership_report,* не ожидая сообщения *membership_query* от маршрутизатора, когда приложение впервые присоединяется к группе рассылки. Сообщения *membership_report* получают маршрутизаторы, а также все хосты, присоединенные к тому же интерфейсу маршрутизатора (например, в случае локальной сети). Каждое сообщение *membership_report* содержит групповой



адрес той группы, в которую вступил отвечающий хост. Обратите внимание, что маршрутизатору все равно, *который* из хостов присоединился к данной группе рассылки или даже *сколько* хостов из данной локальной сети присоединилось к определенной группе. Поскольку маршрутизатор беспокоится лишь о том, принадлежит ли любой из присоединенных к нему хостов к той или иной группе рассылки, в идеальном случае хотелось бы получать не более чем по одному уведомлению о принадлежности к группе. Для этого в протоколе IGMP есть специальный механизм, предназначенный для снижения количества сообщений *membership_report* в том случае, когда несколько присоединенных хостов относятся к одной группе рассылки.

Таблица 6.3.

Типы сообщений протокола IGMP v2

| Тип сообщения | Отправитель | Назначение |
|---|---|---|
| membership_query (общий запрос) | Маршрутизатор | Запрос о группах рассылки, в которые входят присоединенные хосты |
| membership_query (конкретный запрос) | Маршрутизатор | Запрос о том, есть ли среди присоединенных хостов члены указанной группы |
| membership_report | Хост | Уведомление хоста, желающего присоединиться к определенной группе рассылки |
| leave_group | Хост | Уведомление хоста, желающего покинуть определенную группу рассылки |

В частности, каждое посланное маршрутизатором сообщение *membership_query* также содержит поле максимального времени отклика (рис.6.10). Получив сообщение *membership_query,* хост выжидает в течение случайного периода времени в диапазоне от нуля до максимального времени отклика, прежде чем ответить сообщением *membership^report.* Если за время ожидания хост заметит, что сообщение *membership_report* послал какой-либо другой хост, входящий в данную группу рассылки, он воздерживается от

# 7. ПРОТОКОЛЫ ТРАНСПОРТНОГО УРОВНЯ TCP/IP

## 7.1. Функции транспортного уровня

Транспортный уровень предоставляет услуги непосредственно прикладным процессам, выполняющимся на оконечных системах. Протокол транспортного уровня обеспечивает логическое соединение между прикладными процессами, выполняющимися на разных хостах (см.рис.7.1)[58].

С точки зрения приложений, логическое соединение – канал, непосредственно соединяющий процессы, хотя реальная связь между процессами может осуществляться с помощью длинной цепи маршрутизаторов и разнообразных линий связи. Логическое соединение позволяет процессам обмениваться данными, независимо от физической инфраструктуры.

Протоколы транспортного уровня поддерживаются оконечными системами, но не поддерживаются маршрутизаторами. Маршрутизаторы обрабатывают сообщения сетевого уровня и не оказывают влияния на сообщения транспортного уровня.

В Интернет (в любой компьютерной сети, поддерживающей протокол TCP/IP) существуют два протокола транспортного уровня – протокол UDP (User Datagram Protocol – протокол пользовательских дейтаграмм) и протокол TCP (Transmission Control Protocol – протокол управления передачей). Протокол UDP предоставляет приложениям службу ненадёжной передачи данных без установления логического соединения, напротив, протокол TCP предоставляет службу надёжной передачи данных с установлением логического соединения. Создавая новое приложение, разработчик должен выбрать один из двух протоколов транспортного уровня для своего продукта.

Основная задача протоколов UDP и TCP обеспечение обмена данными между процессами, выполняющимися на оконечных системах, при помощи службы обмена данными между оконечными системами, предоставляемой протоколом сетевого уровня (IP). Такое «продолжение» соединения между оконечными системами до уровня процессов называется мультиплексированием и демультиплексированием на транспортном уровне.

[58] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



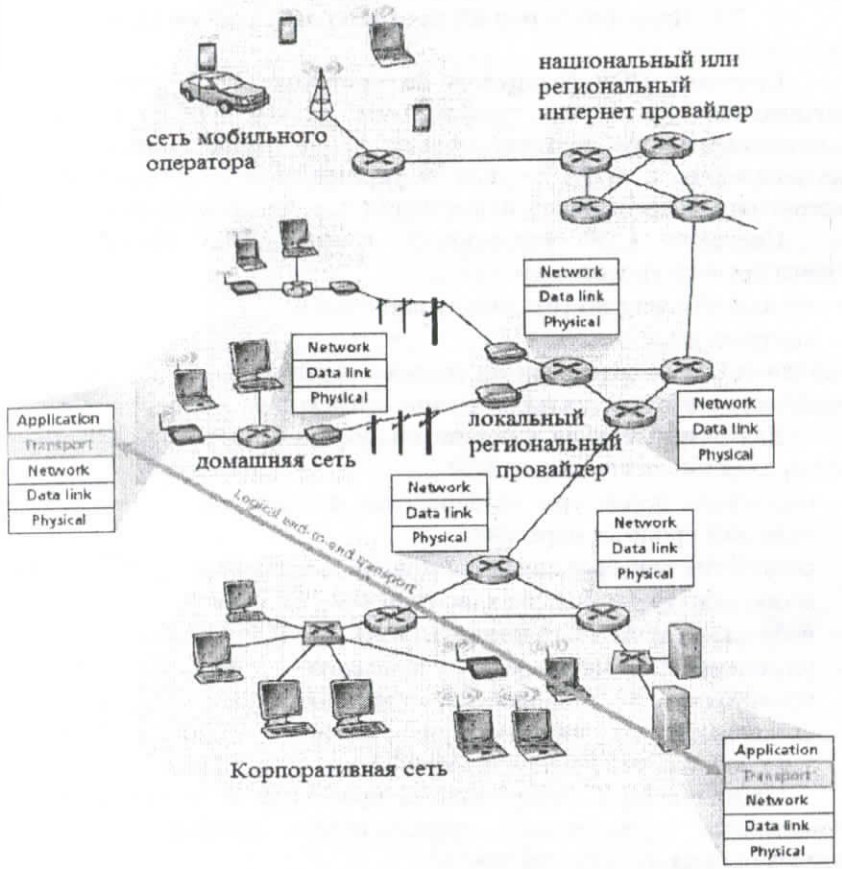



Рис.7.1. Транспортный уровень обеспечивает логическое, а не физическое соединение между прикладными процессами

Подробно данные процедуры описаны в книге J.Kurose, K.Ross. Computer networking ATop-Down Approach[59]. Протоколы UDP и TCP также обеспечивают отсутствие искажений данных при передаче, включая в свои заголовки поля обнаружения ошибок.

[59] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

## 7.2. Пользовательский протокол дейтаграмм UDP

Протокол UDP базируется на протоколе IP и предоставляет прикладным процессам транспортные услуги. Он обеспечивает негарантированную доставку данных, т.е. не требует подтверждения их получения, а также не требует установления соединения между источником и приемником информации, т. е. между модулями UDP.

Протокол UDP гарантирует минимальный набор служб транспортного уровня, а именно:

- служба обмена данными между процессами,
- контроль ошибок

Протокол UDP не контролирует трафик – передача данных может производиться с любой скоростью в течение сколь угодно долгого времени.

Для разработчиков интернет-приложений протокол UDP имеет четыре преимущества перед TCP:

- отсутствие процедуры установления соединения – уменьшается задержка процесса передачи;
- отсутствие информации о состоянии соединения – UDP сервер может обслужить больше клиентов, чем TCP сервер;
- небольшой размер заголовка – UDP 8байт, TCP 20байт;
- улучшенный механизм управления передачей данных приложением – приложения реального времени налагают ограничение на минимальную скорость передачи данных – задержка голосового пакета менее 150мс

Протокол UDP базируется на протоколе IP и предоставляет прикладным процессам транспортные услуги, немногим отличающиеся от услуг протокола IP.

К заголовку IP-пакета протокол UDP добавляет служебную информацию в виде заголовка UDP-пакета (рис.7.2).

| Порт отправителя | Порт получателя |
|---|---|
| Длина | Контрольная сумма |
| Данные | |
| ... | |

Рис.7.2. Формат UDP-пакета

*Порт отправителя (Source Port)* - поле указывает порт рабочей станции, передавшей дейтаграмму. На этот порт следует адресовать



ответную дейтаграмму. Если данное поле не используется, оно заполняется нулями.

*Порт получателя (Destination Port)* - поле идентифицирует порт рабочей станции, на которую будет доставлен пакет.

В среде клиент/сервер Интернет на базе TCP/IP, сервер назначает порты с учётом протокола прикладного уровня, который выполняется на клиентском уровне. Номер порта – это 16-битовые величины в диапазоне от 0 до 65 536. Общеизвестные порты используются системными процессами или прикладными программами, нумеруются числами из диапазона от 0 до 1 023. Например, порт 25 - протокол SMTP (Простого протокола пересылки почты), порт 80 - протокола HTTP.

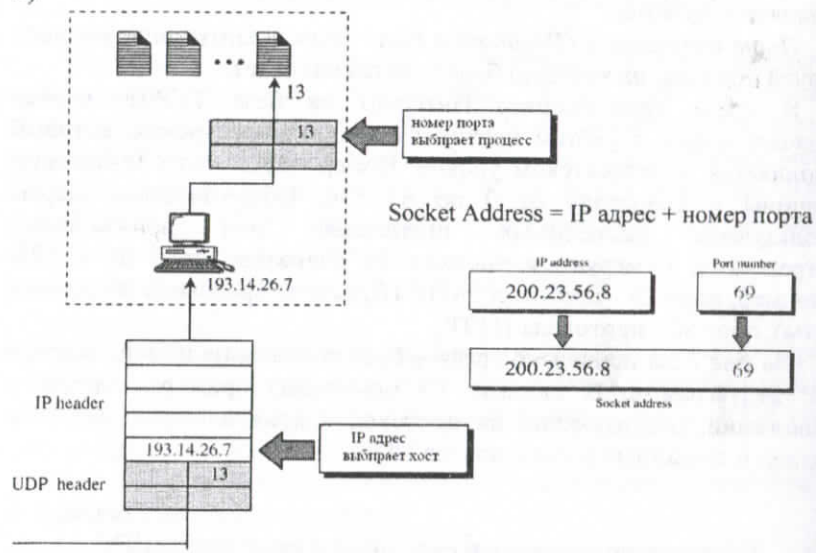
На рис.7.3,а приведено графическое толкование номера порта в UDP дейтаграмме. В таблице 7.1 приведены примеры интернет-приложений, реализующих их протоколов прикладного и сетевого уровней и связанных с ними портов UDP.

Таблица 7.1.

Интернет-приложения и связанные с ними порты UDP

| Приложение | Протокол прикладного уровня | Протокол транспортного уровня | Порт |
|---|---|---|---|
| Email | SMTP | TCP | |
| WWW | HTTP | TCP | |
| File transfer | FTP | TCP | |
| Remote File server | NFS | UDP | |
| IP телефония | H.323 | UDP | 1719 |
| IP телефония (IMO, Skype) | SIP | UDP | 5060 |
| Domain Name Service | DNS | UDP | 53 |
| Simple Network Management Protocol | SNMP | UDP | 161 |

а)




б)

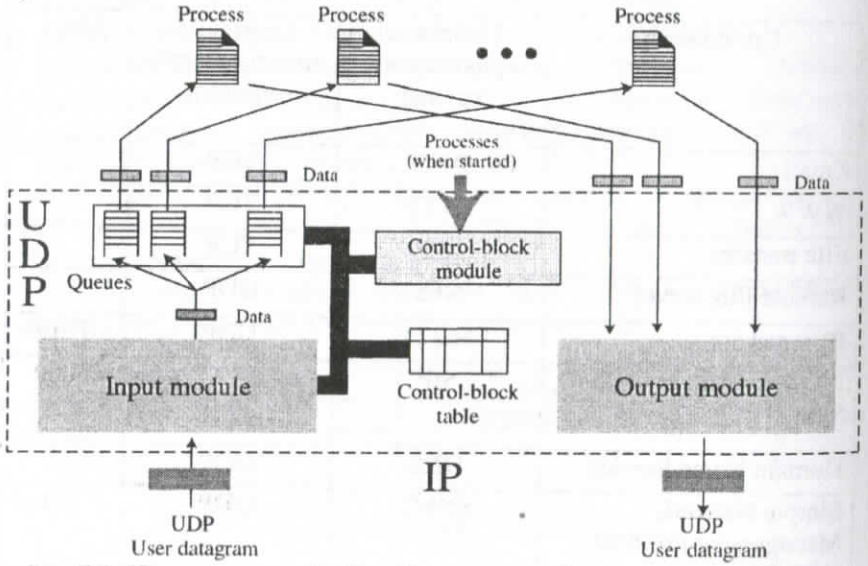



Рис.7.3. Номер порта в UDP дейтаграмме и функциональные блоки UDP



Модуль IP, реализованный в принимающей рабочей станции, передает поступающий из сети IP-пакет модулю UDP (см.рис.7.3,б), если в заголовке этого пакета указано, что протоколом верхнего уровня является протокол UDP. При получении пакета от модуля IP модуль UDP проверяет контрольную сумму, содержащуюся в его заголовке. Если контрольная сумма равна нулю, значит, отправитель ее не подсчитал. Протоколы UDP и TCP имеют один и тот же алгоритм вычисления контрольной суммы (RFC-1071), но механизм ее вычисления для UDP-пакета имеет некоторые особенности. В частности, UDP-дейтаграмма может содержать нечетное число байтов, и в этом случае к ней, для унификации алгоритма, добавляется нулевой байт, который никуда не пересылается.

Более подробную информацию о протоколе UDP можно найти в RFC-768.

### 7.2.1. Контрольная сумма UDP сегмента

Контрольная сумма UDP охватывает UDP заголовок и UDP данные. Контрольная сумма в IP заголовке охватывает только IP заголовок - она не охватывает данные, находящиеся в IP-пакете. И UDP, и TCP содержат контрольные суммы в своих заголовках, которые охватывают как заголовок, так и данные. Для UDP контрольная сумма необязательна, но для TCP она обязательна.

Контрольная сумма UDP рассчитывается точно так же, как контрольная сумма IP заголовка (сумма 16-битных слов с переполнением), хотя существуют и отличия. UDP дата-грамма может состоять из нечетного количества байт, тогда как при расчете контрольной суммы складываются 16-битные слова. При этом в конец датаграммы добавляются нулевые байты заполнения, если это необходимо для расчета контрольной суммы (байты заполнения не передаются).

В UDP и TCP существуют 12-байтовые псевдозаголовки (в UDP датаграммах и TCP сегментах) только для расчета контрольной суммы. Псевдозаголовки содержат в себе определенные поля из IP заголовка. Все это сделано для двойной проверки того, что данные достигли того пункта назначения, которому предназначались (IP не принимает датаграммы, которые не адресованы для данного устройства, и не сможет передать UDP датаграммы, предназначенные для другого верхнего уровня).

Если длина UDP датаграммы нечетная, требуется дополнительный байт для расчета контрольной суммы. Если рассчитанная контрольная сумма равна 0, она хранится как все единичные биты (65535), эти значения эквивалентны в арифметике с поразрядным дополнением (дополнение единицы - ones-complement). Если переданная контрольная сумма равна 0, это означает, что отправитель не рассчитал контрольную сумму.

Если отправитель все же рассчитал контрольную сумму, а получатель определил наличие ошибки, UDP датаграмма уничтожается, сообщение об ошибке не генерируется. (То же самое происходит, если IP уровень обнаружил ошибку в контрольной сумме IP заголовка.)

Контрольная сумма UDP рассчитывается отправителем и проверяется получателем. Она позволяет определить любые изменения в UDP заголовке или данных, которые произошли на пути между отправителем и получателем.

Несмотря на то, что для UDP контрольная сумма - необязательный параметр, она должна рассчитываться всегда. В конце 1980г.г. XXв. некоторые производители компьютеров стали по умолчанию отключать расчет контрольной суммы UDP, чтобы увеличить скорость работы сетевой файловой системы (NFS - Network File System), которая использует UDP. Это может быть допустимым в одной локальной сети, где рассчитывается циклический избыточный код для фреймов на канальном уровне, с помощью которого можно определить повреждение фрейма, когда датаграмма проходит через маршрутизаторы. Существуют маршрутизаторы, у которых есть ошибки в программном или аппаратном обеспечении и которые изменяют биты в датаграммах, которые они маршрутизируют. Эти ошибки не могут быть выявлены в UDP датаграммах, если отключена опция контрольной суммы. Также необходимо отметить, что некоторые протоколы канального уровня (например, SLIP) не имеют каких-либо форм расчета контрольной суммы для данных в канале.

Требования к устройствам Host Requirements RFC требуют, чтобы расчет контрольной суммы UDP был включен по умолчанию. Также они требуют, чтобы принятая контрольная сумма обязательно проверялась, если ее рассчитал отправитель (в том случае, если принятая контрольная сумма не нулевая).



## 7.3. Протокол управления передачей TCP

### 7.3.1. Принципы надежной передачи данных и TCP-соединение

Протокол TCP предоставляет службу надёжной передачи данных с установлением логического соединения. Проблема надежной передачи данных является одной из центральных для компьютерных сетей и проявляется не только на транспортном, но также на сетевом и прикладном уровнях.

На рис.7.4 приведена схема надежной передачи данных. Служба надежной передачи данных обслуживает канал, по которому осуществляется надежная передача сообщений верхних уровней коммуникационной модели[60]. При надежной передаче не происходит искажений битов, то есть изменений их значений с 0 на 1 или наоборот; кроме того, данные доставляются в том порядке, в котором они были отправлены. Именно такая модель обслуживания используется протоколом TCP.

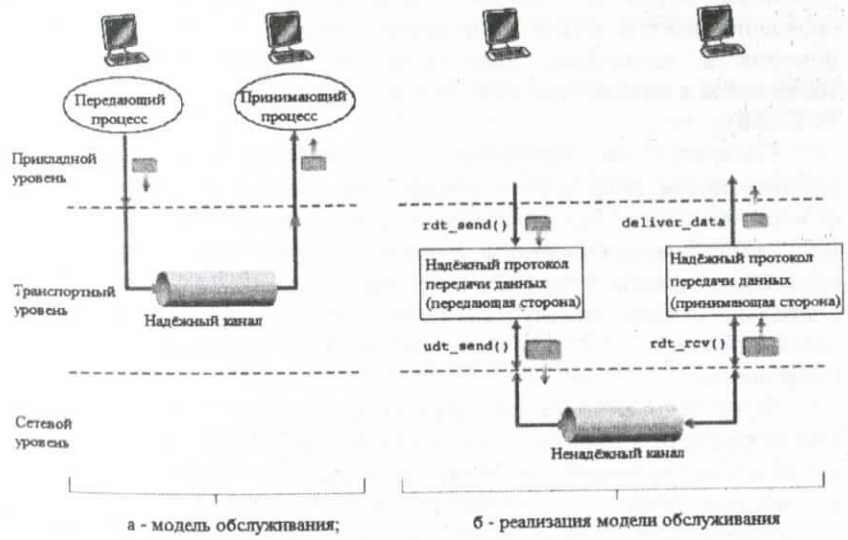



Рис.7.4. Надежная передача данных

[60] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

Главная проблема обеспечения надежной передачи данных протоколом транспортного уровня заключается в том, что протокол более низкого уровня может не поддерживать надежную передачу. Подобная ситуация характерна для протокола TCP, который использует службу ненадежной передачи протокола сетевого уровня IP. Тем не менее, эта проблема может касаться не только транспортного, но сетевого и даже канального уровней: они используют службы передачи данных сетей и отдельных линий связи, которые очевидно не являются надежными.

В этом разделе мы ограничимся лишь *однонаправленной*, или *полудуплексной*, передачей данных, то есть передачей от источника к приемнику. Несмотря на свое название, однонаправленная передача предусматривает движение пакетов в обоих направлениях, как и показано на рис.7.4. Принимающей и передающей сторонам необходимо, кроме данных, обмениваться также различной управляющей информацией.

В протоколе TCP используются многие из методов обеспечения надежной передачи данных: обнаружение ошибок, повторные передачи пакетов, общие квитанции, таймеры и поля порядковых номеров в заголовках пакетов и квитанциях. Описание TCP содержится в документах RFC 793, RFC 1122, RFC 1323, RFC 2018 и RFC 2581.

Говорят, что протокол TCP осуществляет передачу с установлением логического соединения, поскольку перед началом обмена данными два процесса осуществляют «рукопожатие» — процедуру, заключающуюся в передаче друг другу специальных сегментов, предназначенных для определения параметров обмена данными. Частью процедуры установления TCP-соединения является инициализация переменных состояния, связанных с TCP-соединением.

TCP-соединение не является «соединением» в том смысле, в каком этот термин употребляется в коммутируемых сетях. Оно также не является виртуальным каналом, поскольку наблюдение за его состоянием ведется обеими сторонами. Поскольку протокол TCP выполняется на оконечных системах и не выполняется на промежуточных сетевых устройствах (маршрутизаторах и мостах), последние не отслеживают состояния TCP-соединения. Более того, маршрутизаторы не «знают» о существовании TCP-соединения: их работа выполняется на уровне дейтаграмм.



TCP-соединение обеспечивает дуплексную передачу данных. Если на двух хостах выполняются соответственно процессы A и B, то данные могут одновременно передаваться как от процесса A к процессу B, так и от процесса B к процессу A. TCP- соединение также называют соединением **точка-точка**, то есть соединением между единственным приемником и единственным передатчиком.

Рассмотрим процесс установления TCP-соединения. Предположим, что процесс, выполняющийся на одном хосте, желает установить соединение с процессом, выполняющимся на другом хосте. Сначала клиентский процесс сообщает транспортному уровню своего хоста о том, что необходимо установить соединение с серверным процессом. Затем транспортный уровень клиента начинает установление TCP-соединения с транспортным уровнем сервера. Клиент сначала посылает серверу специальный TCP-сегмент, сервер отвечает клиенту другим специальным сегментом, и, наконец, клиент посылает серверу третий специальный сегмент. Первые два сегмента не содержат данных прикладного уровня; третий сегмент может содержать их. Поскольку обмен сегментами входит в процедуру установления соединения, последнюю часто называют *тройным рукопожатием.*

После того как TCP-соединение установлено, прикладные процессы могут начинать обмен данными. Передача данных от клиента к серверу происходит следующим образом: клиент направляет поток своих данных в сокет. Через сокет данные попадают в протокол TCP, выполняющийся на стороне клиента. Как показано на рис.17.2, TCP направляет эти данные в буфер передачи — один из буферов, создаваемых при выполнении тройного рукопожатия. Время от времени TCP извлекает данные из буфера передачи. Согласно спецификации, протокол TCP должен «передать эти данные в виде сегментов в любой подходящий для этого момент времени». Максимальный объем данных, который может быть извлечен из буфера и помещен в сегмент, ограничивается *максимальным размером сегмента* (Maximum Segment Size, MSS). Максимальный размер сегмента данных зависит от реализации протокола TCP (определяется операционной системой) и может быть сконфигурирован; наиболее часто используются значения 1500,536 и 512 байт (размер сегмента данных часто устанавливается так, чтобы избежать IP-фрагментации). Обратите внимание на то, что максимальный размер относится к данным приложения,

содержащимся в сегменте, а не к сегменту вместе с заголовком.

Протокол TCP добавляет заголовок к каждому фрагменту данных, формируя **TCP- сегменты**. Сегменты передаются сетевому уровню, где заключаются в IP-дейтаграммы. Дейтаграммы пересылаются по сети и принимаются получателем. Когда сегмент оказывается на транспортном уровне, протокол TCP помещает данные сегмента в приемный буфер (см.рис.7.5)[61]. Затем приложение считывает поток данных из буфера. Приемный и передающий буферы имеются на обеих сторонах соединения.

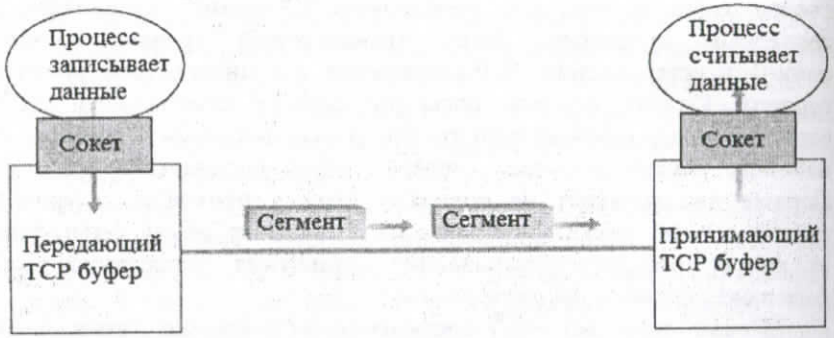



Рис.7.5. Передающий и приемный буферы протокола TCP

Итак, TCP-соединение состоит из буферов и переменных на передающей и принимающей сторонах, а также сокетного соединения между сторонами. При этом для соединения не выделяется никаких буферов или переменных на промежуточных сетевых устройствах (маршрутизаторах, мостах и повторителях).

### 7.3.2. Структура TCP-сегмента

TCP-сегмент (см.рис.7.6) состоит из поля данных и нескольких полей заголовка. Поле данных содержит фрагмент данных, передаваемых между процессами. Как было показано ранее, размер поля данных ограничивается величиной MSS. Когда протокол осуществляет передачу большого файла (например, изображения,

[61] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



являющегося частью web-страницы), он, как правило, разбивает данные на фрагменты размером MSS (кроме последнего фрагмента, который обычно имеет меньший размер).

Как и в протоколе UDP, заголовок TCP (см.рис.7.6) включает номера портов отправителя и получателя, предназначенные для процедур мультиплексирования и демультиплексирования данных, поле контрольной суммы. Кроме того, в состав TCP-сегмента входят еще некоторые поля.

- 32-разрядные поля *порядкового номера* и *номера подтверждения* необходимы для надежной передачи данных.
- 16-разрядное *окно приема* используется для управления потоком данных содержит количество байтов, которое способна принять принимающая сторона.

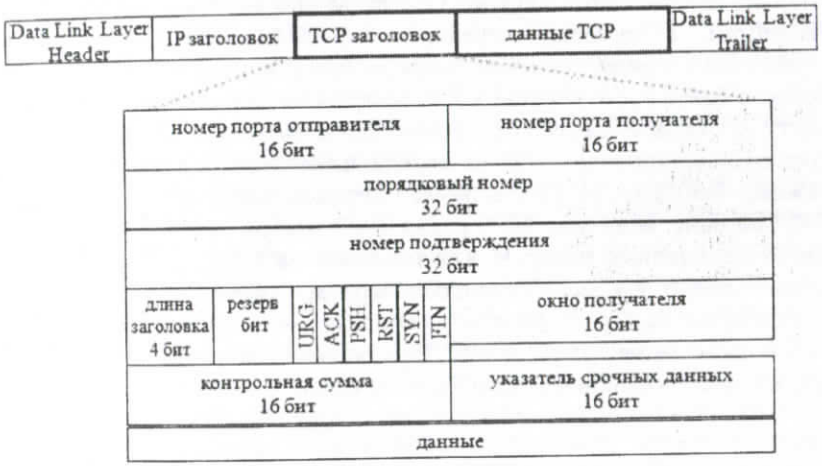



Рис.7.6. Структура TCP-сегмента

- 4-разрядное поле *длины заголовка* определяет длину TCP-заголовка в 32-разрядных словах. TCP-заголовок может иметь переменную длину , обычно длина заголовка составляет 20 байт.
- Необязательное *поле параметров* используется в случаях, когда передающая и принимающая стороны «договариваются» о максимальном размере сегмента, либо для масштабирования окна в высокоскоростных сетях.

существующему TCP-соединению. Заметим, что существующее соединение может использовать те же номера портов, что и предыдущее.

### 7.3.3. Сценарии работы TCP протокола

Рассмотрим несколько ситуаций и соответствующих режимов работы протокола TCP.

**Сценарий «Повторная передача, вызванная потерей квитанции»**

Первую ситуацию иллюстрирует рис.7.8, где хост А посылает один сегмент хосту В. Предположим, что сегмент имеет порядковый номер 92 и содержит 8 байт данных. После передачи этого сегмента хост А ожидает от хоста В сегмент с номером подтверждения 100. Положим, что сегмент, посланный хостом А, успешно получен, а сегмент хоста В оказывается потерянным. В этом случае происходит истечение интервала ожидания, и хост

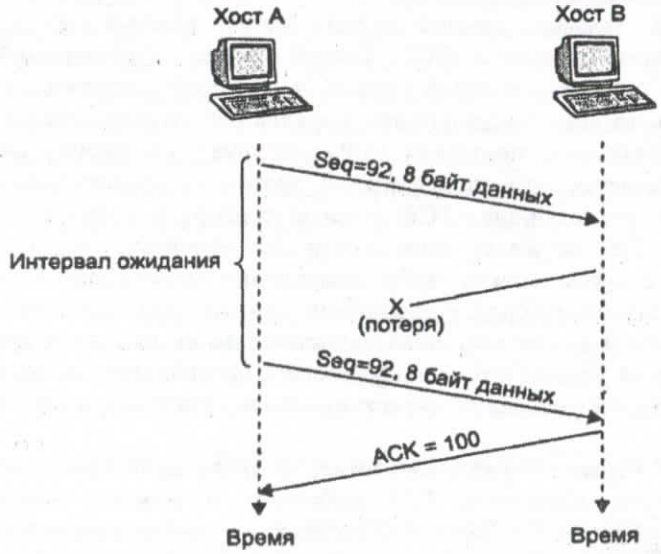



Рис.7.8. Повторная передача, вызванная потерей квитанции



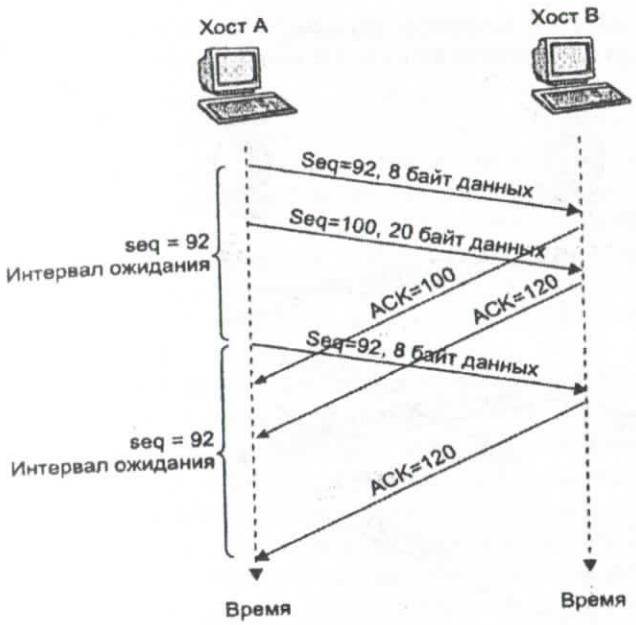



Рис.7.9. Повторная передача сегмента с номером 100 не производится

А отправляет свой сегмент повторно. Хост В получает этот сегмент и по его порядковому номеру выясняет, что такой сегмент им уже принят. Это приводит к удалению повторно переданного сегмента.

**Сценарий «Повторная передача сегмента с номером 100 не производится»**

Вторая ситуация представлена на рис.1. Хост А передает подряд два сегмента, первый из которых имеет порядковый номер 92 и содержит 8 байт данных, а второй сегмент имеет порядковый номер 100 и содержит 20 байт данных. Предположим, что оба сегмента успешно принимаются хостом В, который генерирует две квитанции с номерами подтверждения 100 и 120 соответственно. Пусть ни одна из квитанций не достигает хоста А до истечения интервала ожидания. В этом случае хост А повторно пересылает сегмент с номером 92 и перезапускает таймер. Поскольку хост А получает

квитанцию для второго сегмента до нового истечения интервала ожидания, повторной передачи второго сегмента не происходит.

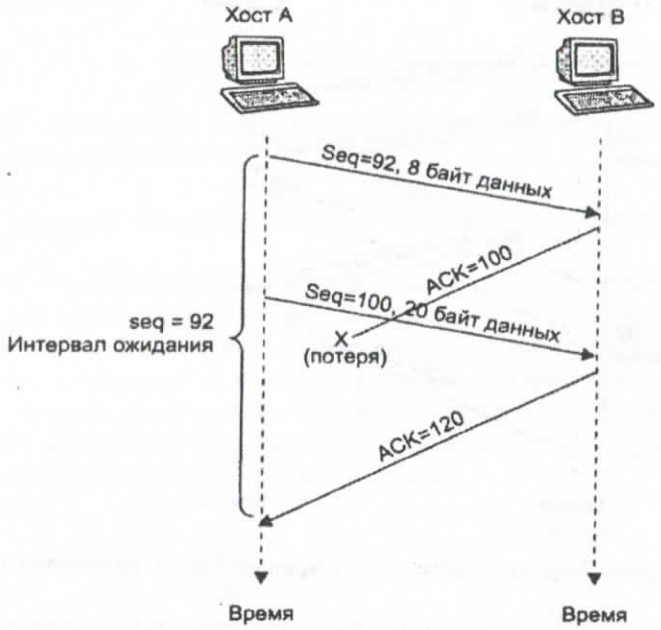



Рис.7.10. Общая квитанция позволяет избежать повторной передачи первого сегмента

### Сценарий «Общая квитанция позволяет избежать повторной передачи первого сегмента»

Третья ситуация приведена на рис.7.10 и отличается от второй тем, что квитанция для первого из сегментов теряется, а вторая квитанция (с номером подтверждения 120) достигает хоста A до истечения интервала ожидания. Получение этой квитанции хостом A сигнализирует о том, что все байты до 119 включительно успешно получены хостом B; таким образом, хосту A не требуется повторно пересылать ни один из двух сегментов.



## 7.4. Управление TCP-соединением

В этом подразделе мы рассмотрим вопросы установления и разрыва TCP-соединения. Процедура установления TCP соединения способна в значительной степени увеличить время ожидания (например, при навигации в web). Пусть процесс, выполняющийся на одном хосте (клиент), желает инициировать соединение с процессом, выполняющимся на другом хосте (с сервером). Сначала клиентское приложение уведомляет TCP-клиент о том, что необходимо установить TCP-соединение с сервером. TCP- клиент инициирует TCP-соединение следующим образом.

- Клиентская сторона TCP отсылает серверной стороне специальный сегмент, не содержащий данных. Флаг SYN, находящийся в заголовке этого сегмента (см. рис.7.11), установлен в 1, поэтому данный сегмент часто называют *SYN- сегментом.* Клиентская сторона устанавливает начальный порядковый номер **(clientjsn)** и помещает его в поле порядкового номера SYN-сегмента. SYN-сегмент заключается в IP-дейтаграмму и отправляется серверу.
- Когда IP-дейтаграмма с SYN-сегментом достигает хоста сервера (если не происходит ее потери), сервер извлекает из нее SYN-сегмент, создает буфер и переменные для соединения, а затем отправляет клиенту сегмент, уведомляющий о выделении TCP-соединения. Этот сегмент также не содержит прикладных данных, однако его заголовок несет важные сведения. Во-первых, флаг SYN, как и в предыдущем сегменте, установлен в 1. Во-вторых, в поле подтверждения содержится число **clientjsn** + 1. Наконец, в поле порядкового номера сервер указывает свой начальный порядковый номер **serverjsn.** Если бы хосты могли общаться при помощи слов, то содержимое второго сегмента, вероятно, выглядело бы следующим образом: «Я получил Ваш SYN-сегмент с просьбой установить с Вами TCP-соединение с начальным порядковым номером **clientjsn.** Я согласен удовлетворить эту просьбу. Мой начальный порядковый номер **serverjsn».** Иногда второй сегмент называют *SYNACK-сегментом.*

3. Получив SYNACK-сегмент, клиент выделяет память для буфера и переменных TCP-соединения и отсылает серверу сегмент, подтверждающий получение SYNACK-сегмента — в поле подтверждения помещается число serverjsn + 1. Поскольку соединение уже установлено, флаг SYN сбрасывается в 0.

После выполнения перечисленных шагов клиент и сервер готовы к обмену данными друг с другом. Во всех последующих сегментах значение флага SYN равно 0. Процесс установления TCP-соединения иллюстрирует рис.7.11. Поскольку в этом процессе клиент и сервер обмениваются тремя сегментами, процедуру установления соединения часто называют *тройным рукопожатием*.


Рис.7.11. Обмен сегментами при тройном рукопожатии в протоколе TCP

Процедура закрытия TCP-соединения подразумевает освобождение памяти, выделенной для буферов и переменных, и может происходить по инициативе любой из сторон. Так, рис.7.12 иллюстрирует закрытие TCP-соединения клиентской стороной. Клиентский процесс генерирует команду закрытия соединения, которая приводит к отправке TCP-клиентом специального сегмента. В заголовке этого сегмента флаг FIN установлен в 1. Получив данный сегмент, сервер подтверждает это. Затем сервер отсылает клиенту завершающий сегмент, в котором бит FIN также установлен в 1; в свою очередь, получение этого сегмента подтверждается клиентом. После этого все ресурсы соединения на обеих сторонах освобождаются.




Рис.7.12. Закрытие TCP-соединения

На протяжении жизни TCP-соединения каждая из сторон проходит через серию изменяющихся *TCP-состояний*. На рис.7.13 приведена типичная последовательность TCP-состояний клиентской стороны.

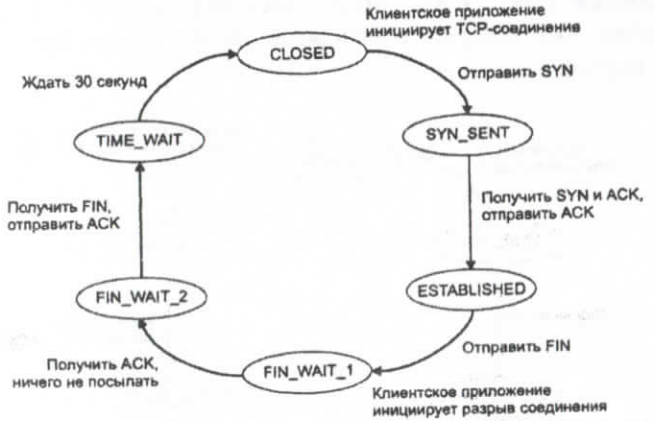



Рис.7.13. Типичная последовательность состояний клиента TCP

Первым состоянием клиента является состояние CLOSED; в этом состоянии происходит инициирование TCP-соединения

клиентским приложением, заключающееся в создании сокета. Клиентская сторона TCP посылает серверной стороне SYN-сегмент и переходит в состояние SYN_SENT. В этом состоянии она ожидает ответного SYNACK-сегмента от сервера, в котором бит SYN установлен в 1. Получив SYNACK-сегмент, клиент входит в состояние ESTABLISHED, в котором он может принимать и отправлять сегменты, содержащие данные прикладного уровня.

Предположим, что закрытие соединения инициируется клиентской стороной (заметим, что сервер также может закрыть соединение). Клиент отправляет TCP- сегмент с битом FIN, установленным в 1, и входит в состояние FIN_WAIT__1. В этом состоянии клиентская сторона ожидает подтверждения (ACK) для переданного сегмента. Получив подтверждение, клиент переходит в состояние FIN_WAIT_2, где ожидает получения от сервера завершающего сегмента с битом FIN, установленным в 1. Получив сегмент, клиент квитирует его и входит в состояние TIME_WAIT. Это состояние предусматривает повторную передачу подтверждения для завершающего сегмента в случае возможной потери этого подтверждения. Длительность нахождения клиента в состоянии TIME_WAIT зависит от реализации протокола, однако наиболее типичными значениями являются 30 с, 1 мин и 2 мин. После выхода из состояния TIME_WAIT происходит формальное закрытие TCP-соединения, при котором освобождаются все его ресурсы, включая номера портов.


Рис.7.14. Типичная последовательность состояний TCP сервера



На рис.7.14 представлена типичная последовательность состояний серверной стороны TCP-соединения для случая, когда закрытие соединения происходит по инициативе клиентской стороны. Переходы из одного состояния в другое понятны, и мы не будем останавливаться на их описании.

### Контрольные вопросы

1. Какие функции выполняет транспортный уровень?
2. Какие протоколы входят в состав транспортного уровня?
3. Какие устройства принадлежат транспортному уровню?
4. Каково назначение протокола UDP?
5. Что входит в заголовок UDP сегмента? Дайте определение порта UDP.
6. Что вы понимаете под мультиплексированием/ демультиплексированием сегментов?
7. Какой из протоколов UDP или TCP обеспечивает ли надежную доставку данных? Каким образом?

Необходимо различать понятия **сетевых приложений** и **протоколов прикладного уровня**. Протоколы прикладного уровня являются частью (хотя и весьма большой) сетевых приложений. Рассмотрим два примера. Web является сетевым приложением, позволяющим пользователям получать web-документы по запросу и состоящим из множества компонентов, включая стандарт формата документов (HTML), браузеры (Netscape Navigator, Microsoft Internet Explorer и др.), web-серверы (например, Apache, Microsoft или Netscape), протоколы прикладного уровня. Протокол прикладного уровня для web носит название протокола передачи гипертекста (HyperText Transfer Protocol, HTTP) и описывает формат и порядок обмена сообщениями между клиентом и сервером (RFC 2646). Таким образом, HTTP является лишь частью web-приложения.

В качестве второго примера рассмотрим приложение электронной почты. Электронная почта Интернета также состоит из множества компонентов: почтовых серверов, содержащих почтовые ящики пользователей, программ для просмотра и создания электронных писем, стандартов, описывающих структуру электронных писем, протоколов прикладного уровня, регламентирующих порядок обмена сообщениями серверов между собой и с оконечными системами пользователей, а также интерпретацию полей, из которых состоят электронные письма. Основным протоколом прикладного уровня для электронной почты является протокол простой передачи сообщений (Simple Mail Transfer Protocol, SMTP). Как мы видим, SMTP (RFC 2821) — лишь часть (хотя и достаточно большая) структуры приложений электронной почты.

Некоторые из протоколов прикладного доступа (HTTP, SMTP и др.) являются официально документированными в RFC. Это означает, что если разработчик нового браузера будет следовать стандарту, то браузер сможет получать документы с любого web-сервера, построенного по этому же стандарту. Тем не менее существует множество протоколов прикладного уровня, которые не стандартизированы и при этом используются для поддержки коммерческих продуктов. В частности, это характерно для Интернет-телефонии.

Сетевое приложение, как правило, состоит из двух «сторон»: **клиентской** и **серверной**. Клиентская и серверная стороны находятся на разных оконечных системах и взаимодействуют путем обмена



сообщениями. Так, web-браузер является клиентской стороной HTTP, в то время как программное обеспечение web-сервера представляет собой серверную сторону протокола. Роль клиентской и серверной сторон для SMTP играют соответственно передающий и принимающий почтовые серверы соответственно.

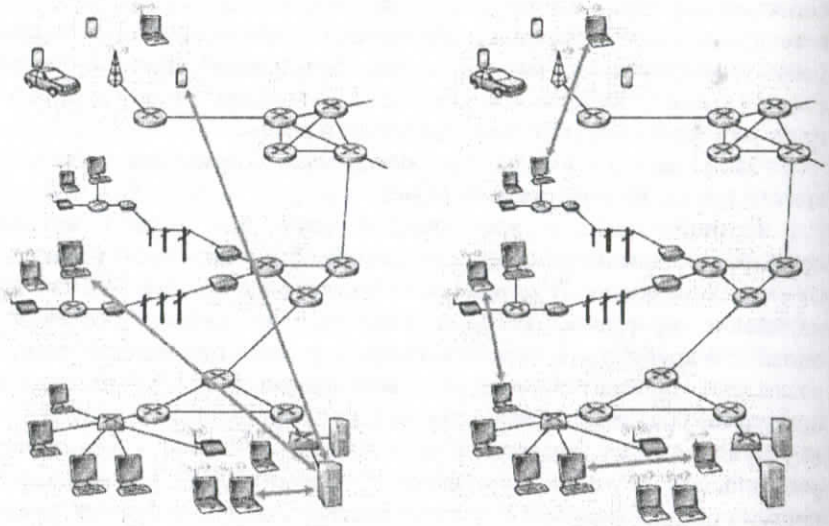
Чаще всего пользуются следующим правилом: клиентом является хост, инициирующий обмен.

Предположим, у вас имеется идея для нового сетевого приложения, давайте рассмотрим, как преобразовать идею в реальное сетевое приложение. В основе развития сетевого приложения является написание программ, которые работают на разных системах и общаются друг с другом по сети. Например, в веб-приложении есть две различные программы, которые взаимодействуют друг с другом: программа браузера, работающая на хосте пользователя (рабочий стол, ноутбук, планшет, смартфон и т. д.); и программа веб-сервера, работающая на хосте веб-сервера. В качестве другого примера, в системе обмена файлами P2P (точка-точка) есть программа на каждом хосте, которая участвует в сообществе обмена файлами. В этом случае программы на разных хостах могут быть похожи или идентичны.

Перед написанием кода программного обеспечения вы должны рассмотреть архитектуру вашего приложения. Необходимо отметить, что архитектура приложения сильно отличается от архитектуры сети. С точки зрения разработчика приложений, сетевая архитектура является фиксированной и предоставляет определенный набор сервисов для приложений. Архитектура приложения, с другой стороны, создана разработчиком приложения и показывает, как приложение структурировано в различных оконечных системах. При выборе архитектуры приложения разработчик приложения будет опираться на одну из двух преобладающих архитектур, используемых в современных сетевых приложениях: архитектуру **клиент-сервер** или **одноранговую P2P** архитектуру (см.рис.8.2)[63].

В архитектуре клиент-сервер, есть постоянно работающий хост, называемый **сервером**, который обслуживает запросы от многих других хостов, называемых **клиентами** (см.рис.8.2,а). Классическим примером этой архитектуры являются известные приложения – WWW, FTP, Telnet и электронная почта.

[63] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



а) Архитектура клиент-сервер б) Архитектура точка-точка

Рис.8.2. Наиболее популярные сетевые архитектуры для разработки и предоставления приложений

В архитектуре клиент-сервер имеется веб-приложение, для которого всегда включенные службы веб-сервера запрашивают данные из браузеров, работающих на клиентских узлах. Когда веб-сервер получает запрос на объект от клиентского узла, он отвечает, отправляя запрошенный объект на клиентский узел. Клиенты напрямую не взаимодействуют друг с другом. Отличительной характеристикой архитектуры является то, что сервер имеет фиксированный, хорошо известный адрес, называемый IP-адресом. Поскольку адрес сервера фиксированный, хорошо известный и сервер всегда включен, клиент всегда может связаться с сервером, отправив пакет на IP-адрес сервера. Часто в приложении клиент-сервер односерверный хост неспособен справляться со всеми запросами от клиентов.

Архитектура **P2P** (pear-to-pear P2P – **точка-точка**) называется одноранговой, т.к. узлы взаимодействуют напрямую друг с другом, запросы и информация, оправляемая и получаемая узлами, не проходит через выделенный сервер (см.рис.8.2,б). В **архитектуре**



**P2P** (pear-to-pear P2P – **точка-точка**) существует минимальная (или нулевая) зависимость от выделенных серверов в центрах обработки данных. Вместо этого приложение использует прямые связи между парами подключенных узлов, называемых точками (peer – точка). **Точки (peers)** не принадлежат поставщику услуг, их роль играют персональные компьютеры и ноутбуки, контролируемые пользователями, большинство **точек (peers)**, расположены в домах, университетах и офисах.

## 8.2. Взаимодействие процессов через сеть

Как было сказано выше, многие приложения состоят из двух «сторон», взаимодействующих друг с другом через компьютерную сеть. Взаимодействие осуществляется путем передачи и приема сообщений. Процесс осуществляет прием и передачу сообщений через свой **сокет**. Сокет можно сравнить с дверью: когда процессу необходимо произвести отправку сообщения, он «выталкивает» сообщение через «дверь», предполагая, что некто снаружи (службы более низких уровней) осуществит доставку сообщения до «двери» адресата. Затем сообщение попадает через «дверь» непосредственно приложению-адресату, которое осуществляет его обработку.

На рис.8.3 изображено взаимодействие двух процессов через Интернет посредством сокетов (хотя в представленной ситуации используется протокол TCP, с тем же успехом это мог бы быть протокол UDP)[64]. Как можно видеть, сокет представляет собой интерфейс между прикладным и транспортным уровнями хоста. Сокет также часто называют прикладным программным интерфейсом (API), осуществляющим связь приложения и компьютерной сети. Под контролем разработчика приложения практически целиком находится часть сокета, относящаяся к прикладному уровню, чего нельзя сказать о его «транспортной» части. Здесь в компетенции разработчика лишь выбор протокола транспортного уровня и установка значений нескольких параметров транспортного уровня (максимальный размер буфера, максимальный размер сегмента и др.). Приложение всегда строится с использованием единственного транспортного протокола.

[64] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

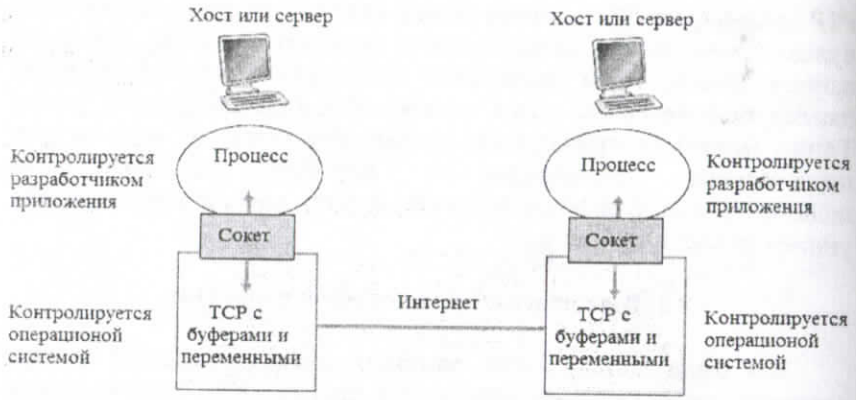



Рис.8.3. Процессы приложения, сокеты и протокол транспортного уровня

Для успешного обмена сообщениями между процессами, выполняющимися на двух различных хостах, необходимо, чтобы они могли идентифицировать друг друга. Идентификация требует наличия следующей информации о процессе:

- имя или адрес хоста, которому принадлежит процесс;
- идентификатор процесса внутри хоста.

В Интернет-приложениях хосты идентифицируются с помощью IP-адресов. IP-адрес представляет собой 32-разрядное двоичное число, уникальное для каждого хоста сети (точнее, это число уникально для каждого интерфейса, с помощью которого осуществляется подключение хоста к сети). IP адреса подробно рассмотрены в разделе 5.5.

Идентификация процесса внутри хоста производится с помощью уникального для каждого процесса хоста *номера порта* (в качестве примера см. раздел 7.2 Таблица 7.1). Популярные Интернет-протоколы прикладного уровня имеют стандартизированные (говорят: *хорошо известные*) значения номеров портов. Так, процесс, использующий протокол HTTP, получает порт номер 80, а процесс, использующий протокол SMTP, — порт номер **25.** Хорошо известные номера портов можно найти в документе **RFC** 1700 (который в настоящее время является несколько устаревшим) и на сайте **http://www.iana.org (RFC 3232).** Когда разработчик создает новое



сетевое приложение, он должен назначить приложению собственный номер порта.

## 8.3. Службы, необходимые приложению

Вспомним, что сокет является интерфейсом между прикладным процессом и протоколом транспортного уровня. На передающей стороне сообщения через сокет оказываются на транспортном уровне, где получают возможность перемещаться внутри сети. Сетевые службы обеспечивают доставку сообщения на транспортный уровень адресата, где оно через сокет попадает в нужное приложение и обрабатывается им. Многие компьютерные сети, включая Интернет, используют более одного транспортного протокола. При разработке приложения необходимо выбрать один из транспортных протоколов, к службам которого оно будет обращаться. Как сделать выбор? Нужно изучить перечень служб, поддерживаемых каждым из протоколов, и выбрать тот, который способен обслужить ваше приложение наилучшим способом. Подобный выбор вы совершаете, решая, следует ли вам воспользоваться в путешествии поездом или самолетом. У каждого вида транспорта есть свои преимущества (например, поезд совершает остановки между конечными пунктами, а самолет тратит меньше времени в пути).

Какие службы могут понадобиться приложению? Выделяются три основных требования, предъявляемых приложениями к транспортному уровню: надежная передача данных, гарантированная скорость передачи и обеспечение доставки данных за определенное время.

### Надежная передача данных

Некоторые приложения, например приложения электронной почты, обмена сообщениями в реальном времени, передачи файлов, просмотра web-документов, финансовых операций и т. д., требуют надежной передачи данных, то есть исключения вероятности потерь данных при передаче. Как правило, потери данных приводят к крайне нежелательным для пользователей последствиям (представьте обмен между банком или его клиентом!). Тем не менее, существует вид приложений, *толерантных к потерям данных*. К нему относится большинство мультимедийных приложений, например аудио и видео

реального времени. Небольшие потери данных в таких приложениях оборачиваются помехами (звуковые щелчки и «дергающееся» изображение), не приводящими к сбоям или серьезным потерям качества. Степень толерантности приложения к потере данных определяет максимальную долю данных, которая может быть потеряна, и, как правило, зависит от назначения приложения и использующейся схемы кодирования.

**Скорость передачи**

Для эффективной работы некоторым приложениям необходимо осуществлять передачу данных с определенной скоростью. Например, если приложение Интернет-телефонии кодирует аналоговые голосовые сообщения в цифровые с интенсивностью 32кбит/с, то для успешного функционирования необходимо обеспечить передачу данных этого приложения со скоростью 32кбит/с. В противном случае между фразами пользователей будут ощущаться задержки. Для избежания таких ситуаций приложение должно либо снизить интенсивность кодирования до величины, согласующейся со скоростью передачи, либо завершить свою работу. Приложения, эффективность которых зависит от скорости передачи данных, называют *чувствительными к скорости передачи данных*. На сегодняшний день многие мультимедиа-приложения являются чувствительными к скорости передачи, однако в будущем ожидается кардинальное усовершенствование систем кодирования, которые позволят приложениям адаптироваться к используемому каналу связи. Такой способностью обладают приложения электронной почты, web-приложения и приложения для передачи файлов, относящиеся к классу *эластичных* приложений. Разумеется, наличие высокоскоростного канала связи никогда не повредит работе сети; здесь весьма актуально утверждение о том, что полоса пропускания никогда не бывает слишком широкой.

**Время передачи**

Последнее требование приложений к транспортному уровню заключается в гарантированном времени доставки данных. Интерактивные приложения реального времени, такие как Интернет-телефония, виртуальные миры, телеконференции и многопользовательские компьютерные игры, накладывают жесткие



временные ограничения на время доставки данных (сотни миллисекунд и менее). Невыполнение временных ограничений в Интернет-телефонии приводит к длительным паузам в разговоре, а в компьютерных играх *- к задержке реакции окружения и, следовательно, к потере реалистичности. В приложениях, не относящихся к приложениям реального времени, временные ограничения на доставку данных не являются столь принципиальными, однако меньшая задержка всегда предпочтительней, чем большая.

В табл.8.1 суммируются требования различных видов приложений к качеству передачи данных. Разумеется, не следует воспринимать эти данные как строгую классификацию; напротив, они отражают лишь тенденции, характерные для того или иного класса приложений.

Таблица 8.1.

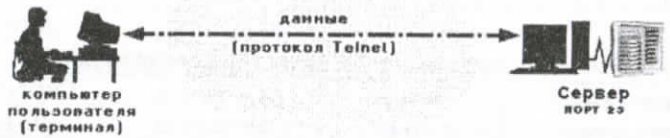
Требования приложений к качеству передачи данных

| Приложение доставки | Потеря данных | Скорость передачи | Ограничение на время |
|---|---|---|---|
| Передача файлов | Недопустима | Эластичность | Нет |
| Электронная почта | Недопустима | Эластичность | Нет |
| Работа с web-документами | Недопустима | Эластичность (несколько Кбит/с) | Нет |
| Аудио и видео реального времени | Допустима | Аудио: несколько Кбит/с-1 Мбит/с, видео: 10 Кбит/с-5 Мбит/с | Есть, сотни миллисекунд |
| Записанное потоковое аудио и видео | Допустима | Аналогично предыдущему | Есть, несколько секунд |
| Интерактивные игры | Допустима | 1-10 Кбит/с | Есть, сотни миллисекунд |
| Обмен сообщениями в реальном времени | Недопустима | Эластичность | Есть и нет |

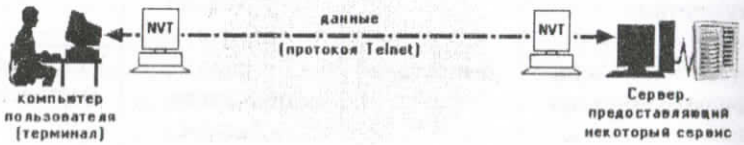
## 8.4. Сервис Telnet – стандартный протокол для услуг виртуального терминала

Сервис *Telnet*-одна из самых старых информационных технологий Internet. В настоящее время этот сервис практически не используется. Поэтому имеет смысл ограничиться изложением только общих принципов организации этого сервиса.

Основным назначением сервиса Telnet является реализация сетевого терминала для доступа к ресурсам удаленного компьютера. Он обеспечивает двунаправленный канал передачи данных (рис.8.4,а)[65].




а)




б)

Рис.8.4. Схема обеспечения сервиса Telnet
а) схема клиент-сервер для сервиса Telnet б) схема сетевого виртуального терминала

В сервисе Telnet используется TCP-соединение для передачи данных и управляющей информации. При этом протокол Telnetдля обеспечения удаленного доступа терминала к серверу резервирует порт 23.

[65] В.П. Комагоров. Технологии сети Интернет: протоколы и сервисы. – Томск: Томский политехнический университет, 2009. – 107с.



Он выполняет три базовые функции:

- определяет сетевой виртуальный терминал (NVT- network virtual terminal), который обеспечивает стандартный интерфейс к удаленной системе;
- включает механизм, который позволяет клиенту и серверу согласовать опции обмена;
- обеспечивает симметрию соединения, создавая любой программе сервера возможность выступать в качестве клиента.

Протокол Telnet позволяет серверу рассматривать все удаленные терминалы как стандартные «сетевые виртуальные терминалы» строчного типа (рис.8.4,б), работающие в кодах ASCII, а также обеспечивает возможность согласования более сложных функций (например, локальный или удаленный эхо-контроль, страничный режим, и т. д.).

Рассмотрим организацию работы сервиса Telnet. На прикладном уровне над Telnet находится либо программа поддержки реального терминала, либо прикладной процесс на сервере, к которому осуществляется доступ с терминала. Формат NTVдостаточно прост. Для данных используются 7-битовые ASCIIкоды. 8-битовые октеты зарезервированы для командных последовательностей.

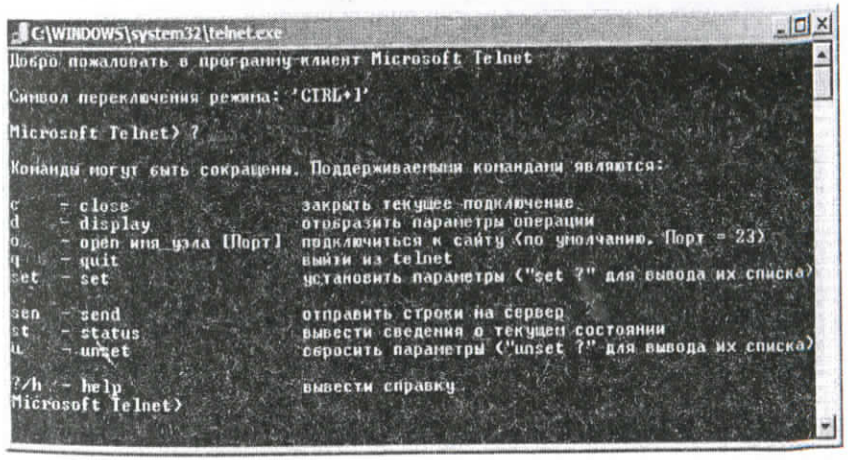



Рис.8.5. Вид окна программы Telnet

Приложения и возможности – Параметры и компоненты – Включение и отключение компонентов Windows – В открывшемся окне находим «Клиент Telnet» и ставим на него галочку (см.рис.8.9).

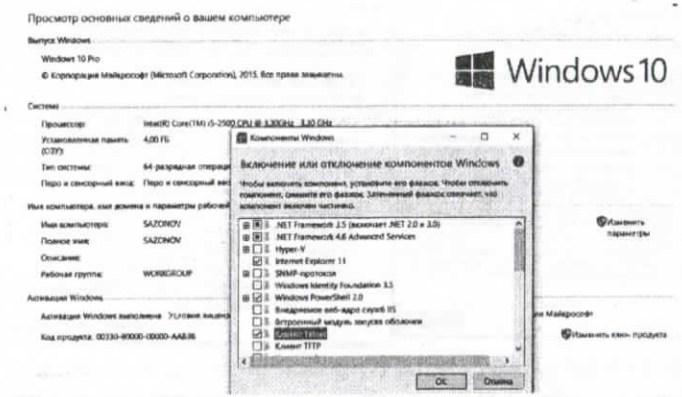



Рис.8.9. Окно Windows10

6. Далее в Windows10 в поиске прописать «telnet 10.62.5.101»

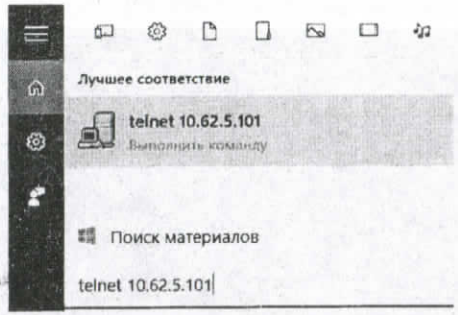



Рис.8.10. Поиск telnet 10.62.5.101 в Windows10

7.В открывшемся окне вводим логин и пароль.

8.В строчке прописываем EN и нажимаем клавишу Enter. Система опять запросит пароль. Вводим пароль и нажимаем клавишу Enter.



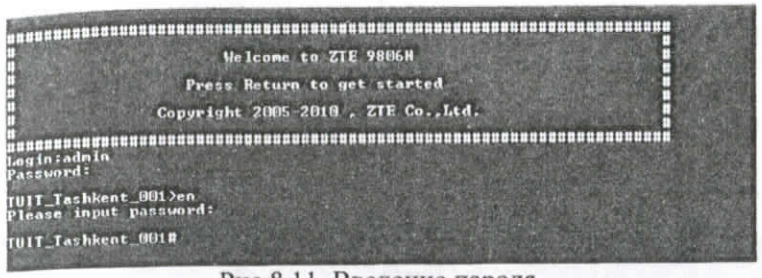



Рис.8.11. Введение пароля

9.Заходим в конфигурацию оборудования. Для этого набираем команду **Configure**.

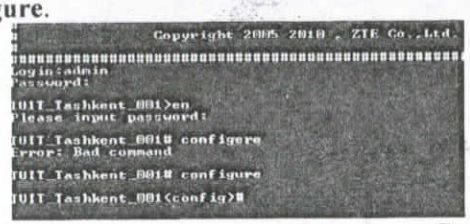



Рис.8.12. Результат выполнения команды Configure

10.Для добавления профиля набираем с клавиатуры:
Adsl-profile (Name), где Name название профиля, в нашем случае это будет выглядить так:
Adsl-profile 2m\1m
нажимаем клавишу Enter до тех пор, пока не перейдем на строчку AtucChanConfFastMaxTxRate(0...102400kbps):[1024]
На этой строчке мы задаем скорость скачивания для нашего профиля. В нашем случае это 2048Мбит/с.

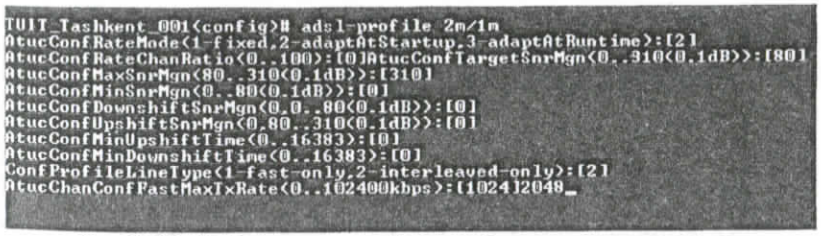



Рис.8.13. Добавление профиля набираем с клавиатуры

И продолжаем нажимать клавишу Enter до строчки
AtucChanConfFastInterleaveTXRate(0...102400kbps):[1024]
тут также прописываем 2048 и нажимаем клавишу Enter до строчки
AturChanConfFastMaxTxRate(0...1024bps):[512].
На этой строчке мы прописываем скорость отдачи (Upload) по заданию у нас 1024кбит/с.

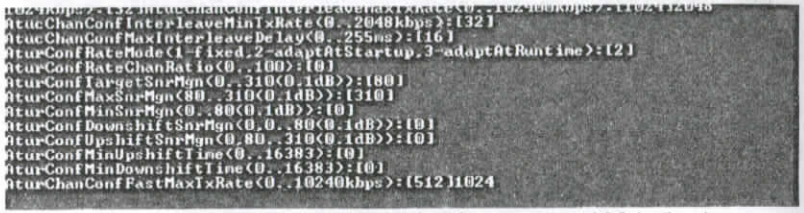



Рис.8.14. Прописывание Upload скорости 1024кбит/с

Нажимаем клавишу Enter строчки
AturChanConfFastInterleaveTXRate(0...1024kbps):[512]
и также ставим 1024 и нажимаем клавишу Enter до тех пор, пока закончится настройка профиля.
Чтобы посмотреть какие профили уже существуют, надо использовать команду Show adsl profile.

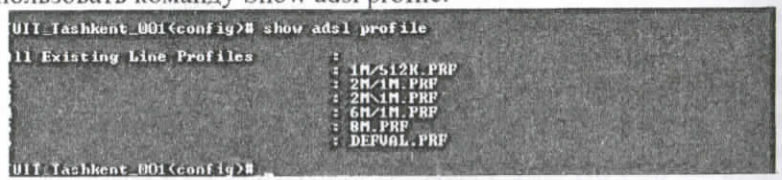



Рис.8.15. Просмотр уже существующих профилей

Как видно из скриншота (рис.8.15) наш профиль создан.
Ниже приведена последовательность команд работы протокола telnet.

TUIT_Tashkent_001 (config)# adsl-profile 2m/1m
TUIT_Tashkent_001 (config)# adsl-profile 2m/1m
AtucConfRateMode(1-fixed,2-adaptAtStartup,3-adaptAtRuntime):[2]
AtucConfRateChanRatio(0..100):[0]
AtucConfTargetSnrMgn(0..310(0.1dB)):[80]
AtucConfMaxSnrMgn(80..310(0.1dB)):[310]



AtucConfMinSnrMgn(0..80(0.1dB)):[0]
AtucConfDownshiftSnrMgn(0..310):[0]
AtucConfUpshiftSnrMgn(0..310):[0]
AtucConfMinUpshiftTime(0..16383):[0]
AtucConfMinDownshiftTime(0..16383):[0]
ConfProfileLineType(1-fast-only,2-interleaved-only):[2]1
AtucChanConfFastMaxTxRate(0..102400kbps):[1024]2048
AtucChanConfFastMinTxRate(0..2400kbps):[32]
AtucChanConfInterleaveMaxTxRate(0..102400kbps):[1024]2048
AtucChanConfInterleaveMinTxRate(0..2400kbps):[32]
AtucChanConfMaxInterleaveDelay(0..255ms):[8]
AturConfRateMode(1-fixed,2-adaptAtStartup,3-adaptAtRuntime):[2]
AturConfRateChanRatio(0..100):[0]
AturConfTargetSnrMgn(0..310(0.1dB)):[80]
AturConfMaxSnrMgn(80..310(0.1dB)):[310]
AturConfMinSnrMgn(0..80(0.1dB)):[0]
AturConfDownshiftSnrMgn(0..310(0.1dB)):[0]
AturConfUpshiftSnrMgn(0..310(0.1dB)):[0]
AturConfMinUpshiftTime(0..16383):[0]
AturConfMinDownshiftTime(0..16383):[0]
AturChanConfFastMaxTxRate(0..10240kbps):[512]1024
AturChanConfFastMinTxRate(0..512kbps):[32]
AturChanConfInterleaveMaxTxRate(0..10240kbps):[512]1024
AturChanConfInterleaveMinTxRate(0..512kbps):[32]
AturChanConfMaxInterleaveDelay(0..255ms):[16]
AtucDMTConfFreqBinsOperType(1-open,2-cancel):[2]
AturDMTConfFreqBinsOperType(1-open,2-cancel):[2]
LineDMTConfEOC(1-byte ,2-streaming ):[1]
LineDMTConfTrellis(1-on,2-off):[1]
AtucConfMaxBitsPerBin(0..15):[15]
AtucConfTxStartBin(6..511):[32]
AtucConfTxEndBin(32..511):[511]
AtucConfRxStartBin(6..63):[6]
AtucConfRxEndBin(6..63):[31]
AtucConfUseCustomBins(1-on,2-off):[2]
AtucConfDnBitSwap(1-on,2-off):[2]
AtucConfUpBitSwap(1-on,2-off):[2]
AtucConfREADSL2Enable(1-on,2-off):[2]
AtucConfPsdMaskType(1-DMT_PSD_MSK,2-ADSL2_PSD_MSK,3-

ADSL2_READSL_WIDE_PSD_MSK,
4-ADSL2_READSL_NARROW_PSD_MSK):[3]
AtucConfPMMode(1-DISABLE,2-L2_ENABLE,3-L3_ENABLE,4-L3_ENABLE | L2_ENABLE):[1]
AtucConfPML0Time(0..255s):[240]
AtucConfPML2Time(0..255s):[120]
AtucConfPML2ATPR(0..31db):[3]
AtucConfPML2Rate(512..1024kbps):[512]

### 8.5. Сервис FTP – система файловых архивов

FTP-сеанс представляет собой обмен файлами, находящимися на двух хостах — локальном и удаленном. Для получения доступа к удаленному хосту пользователю необходимо ввести свои имя и пароль. После получения доступа пользователь может осуществлять передачу файлов как с удаленного хоста на локальный, так и наоборот. Как показано на рис.8.16, пользователь взаимодействует с FTP при помощи пользовательского агента FTP[68]. Сначала пользователь указывает имя удаленного хоста FTP-клиенту для установления TCP-соединения с сервером, а затем вводит свои имя и пароль, пересылаемые серверу при помощи FTP-команд. После распознавания пользователя сервером начинается процесс передачи файлов в нужном направлении.

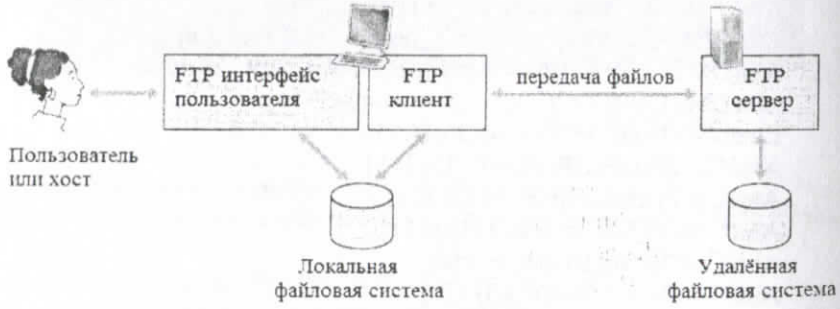



Рис.8.16. FTP осуществляет передачу файлов между локальной и удаленной файловыми системами

[68] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



HTTP и FTP являются протоколами передачи файлов и имеют много общего; например, в качестве протокола транспортного уровня они оба используют TCP. Тем не менее между HTTP и FTP существуют и принципиальные различия. Протокол FTP использует два параллельных TCP-соединения: **управляющее соединение** и **соединение данных**. Управляющее соединение служит для пересылки управляющей информации между двумя хостами: имени пользователя и пароля, команд смены текущего удаленного каталога, передачи и запроса файлов. Соединение данных предназначено для передачи самих файлов. Поскольку управляющее соединение отделено от соединения данных, говорят, что передача управляющей информации осуществляется **вне полосы** (out-of-band). В отличие от FTP, протокол HTTP через единственное TCP-соединение осуществляет передачу и файлов, и команд (строк заголовков для запросов и ответов). Поэтому говорят, что HTTP передает свою управляющую информацию *внутри полосы* (in-band). Другим примером протокола с передачей управляющей информации внутри полосы является SMTP, характерный для приложений электронной почты. Мы рассмотрим протокол SMTP в следующем разделе. На рис.8.17 приведена иллюстрация двух соединений протокола FTP[69].

FTP-сеанс начинается с установления управляющего TCP-соединения между клиентом и удаленным хостом (сервером) через порт с номером 21. По этому соединению осуществляется передача имени пользователя и пароля, а также команд смены текущего каталога и обмена файлами. Когда сервер получает команду передачи или приема файла, он устанавливает с клиентом TCP-соединение данных, затем осуществляет файловый обмен и закрывает соединение. Каждое соединение позволяет передать только один файл; таким образом, множественный обмен вызывает необходимость многократной установки соединения данных. При этом управляющее соединение остается открытым в течение всего сеанса. Учитывая введенную терминологию, соединение данных можно отнести к непостоянным соединениям.

[69] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

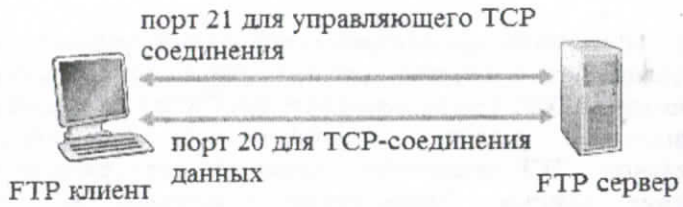



Рис.8.17. Управляющее соединение и соединение данных

Во время FTP-сеанса серверу необходимо иметь информацию о пользователе. Как правило, управляющее соединение связано со специальной учетной записью пользователя. Кроме того, сервер должен следить за текущим каталогом, в котором работает пользователь. Необходимость затрат ресурсов на хранение информации приводит к значительному снижению числа FTP-сеансов, одновременно поддерживаемых сервером. В этом заключается недостаток протокола FTP по сравнению с HTTP: как вы помните, HTTP не запоминает состояние соединения.

## 8.6. Сервис электронная почта (e-mail)

Электронная почта появилась едва ли не раньше Интернета. В эпоху зарождения Интернет-технологий она была самым популярным из существовавших приложений, а за годы развития претерпела множество изменений и продолжает меняться до сих пор.

Как и обычная почта, электронная почта является асинхронным средством связи: люди посылают друг другу сообщения в любое удобное для них время без предварительной договоренности с адресатами. Преимуществами электронной почты перед обычной являются высокая скорость доставки, простота использования и низкая стоимость обслуживания. С помощью списка рассылки с адресами отправитель может разослать одно и то же письмо сотням получателей одновременно. Кроме того, современная электронная почта позволяет вместе с письмами пересылать гиперссылки, текст в формате HTML, изображения, аудио- и видеофайлы, Java-апплеты и т.д.



На рис.8.18 представлена структура системы электронной почты[70]. В этой структуре можно выделить три ключевых компонента: **агенты пользователя**, **почтовые серверы** и **протокол SMTP**. Мы рассмотрим каждый из компонентов на примере двух пользователей, Алисы и Алекса, общающихся по электронной почте. Агенты пользователя позволяют читать, отвечать, пересылать, создавать и сохранять электронные письма; их часто называют программами для чтения почты, хотя мы постараемся избегать этого термина в нашей книге. Когда Алиса создает новое письмо Алексу, ее агент отсылает письмо почтовому серверу, где письмо попадает в очередь исходящих сообщений сервера. Когда Алекс захочет прочитать письмо, его агент соединится с почтовым сервером и доставит письмо на персональный компьютер Боба. Во второй половине 1990г.г. XXв. большое распространение получили агенты с графическим интерфейсом пользователя (Graphical User Interface, GUI), позволяющие читать и создавать мультимедийные сообщения.

Теперь рассмотрим подробнее, каким образом осуществляется передача сообщения между почтовыми серверами. Любопытно отметить, что протокол SMTP по своей сути напоминает непосредственное общение между двумя людьми. Итак, сначала SMTP-клиент пытается установить TCP-соединение с портом 25 сервера; если сервер не отвечает, попытка повторяется позднее. После того как соединение установлено, клиент и сервер обмениваются рукопожатиями на прикладном уровне по аналогии с людьми, которые представляются друг другу перед тем, как начать общение. В ходе процедуры рукопожатия клиент определяет адреса почтовых ящиков отправителя и получателя сообщения. По завершении рукопожатия начинается процесс передачи сообщения от клиента к серверу.

Поскольку передача осуществляется с помощью протокола TCP, гарантируется надежная доставка данных. Если в очереди клиента имеются другие сообщения, предназначенные этому же серверу, все они пересылаются последовательно через одно TCP-соединение. После передачи всех сообщений клиент закрывает соединение с сервером.

[70] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

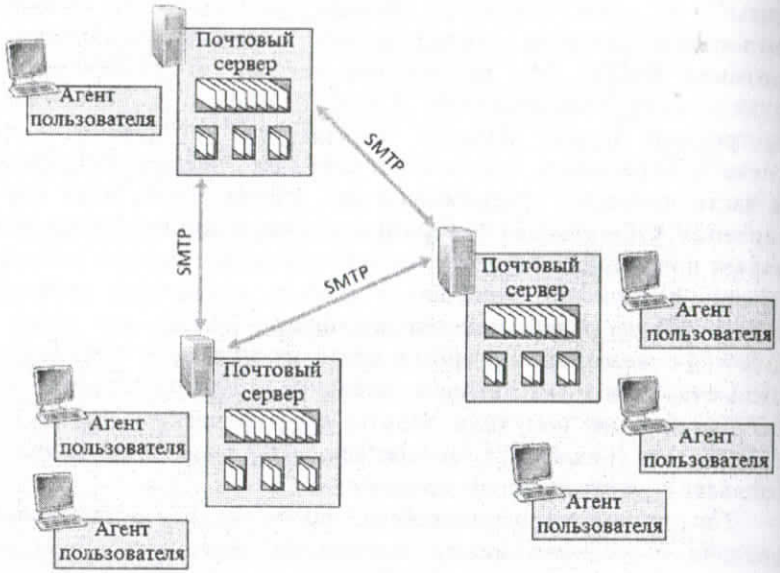



Рис.8.18. Структура электронной почты Интернета

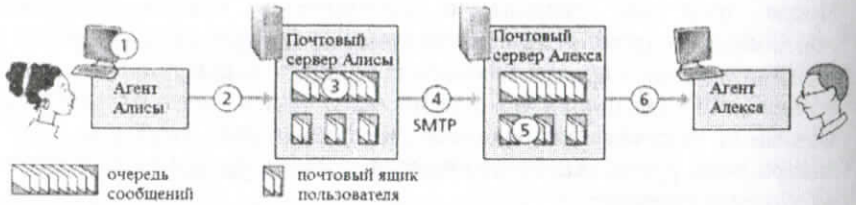



Рис.8.19. Алиса посылает сообщение Алексу

### 8.6.1. Сравнение SMTP и HTTP

Теперь настало время сравнить два важных Интернет-протокола: HTTP и SMTP. Оба они предназначены для передачи файлов между хостами, при этом HTTP организует передачу объектов между web-клиентом (который обычно представляет собой



браузер) и web-сервером, а SMTP — передачу электронных сообщений между двумя почтовыми серверами. Как HTTP, так и SMTP используют постоянные соединения. Тем не менее, наряду с описанными сходствами, протоколы обладают и различиями, описанными ниже.

1. HTTP представляет собой **протокол получения** (pull protocol), то есть некто загружает на web-сервер нужную информацию, которую пользователи с помощью протокола HTTP **получают** с сервера в удобное для себя время. Как правило, TCP-соединение устанавливается компьютером, инициирующим получение файла. SMTP, напротив, является **протоколом отправки** (push protocol), то есть передающий почтовый сервер **отправляет** файл принимающему почтовому серверу. Как правило, TCP-соединение устанавливается компьютером, инициирующим отправку файла.
2. SMTP требует 7-разрядной кодировки ASCII для символов в заголовке и теле каждого сообщения. Если сообщение содержит символы расширенной кодировки ASCII (например, символы национальных алфавитов) или бинарные данные, требуется преобразование таких данных в 7-разрядную кодировку ASCII. Протокол HTTP не накладывает подобных ограничений на сообщения.
3. протоколы SMTP и HTTP поддерживают разные способы обработки документов, содержащих текстовую и графическую (или мультимедийную) информацию. Как будет описано в разделе «Web и HTTP», протокол HTTP пересылает каждый объект в отдельном ответном сообщении; SMTP, напротив, помещает все объекты в одно сообщение.

### 8.6.2. Форматы сообщений электронной почты и MIME

Когда Алиса пишет обычное электронное письмо Алексу, она может снабдить его различной дополнительной информацией: почтовым адресом Алекса, своим почтовым адресом, датой создания письма. Подобная информация содержится в заголовке письма, предшествующем его телу. Заголовок представляет собой совокупность строк, которые описаны в документе RFC 822. Заголовок сообщения отделяется от тела пустой строкой (CRLF). RFC 822 определяет формат всех строк заголовка сообщения, а также их семантическую интерпретацию. Как и в протоколе HTTP, каждая строка заголовка содержит текст в виде символов ASCII, вклю-

чающий ключевое слово и значение, разделенные знаком двоеточия. Некоторые ключевые слова являются обязательными, другие — не обязательными. Примерами обязательных ключевых слов являются From: и To:, а не обязательных — Subject:. Обратите внимание на то, что строки заголовка отличаются от SMTP-команд, рассмотренных ранее в этом разделе. Команды представляют собой часть процедуры рукопожатия, а строки заголовка — часть передаваемого сообщения.

Типичный заголовок сообщения выглядит следующим образом:

From: alice@crepes.fr
To: alex@hamburg.edu
Subject: Searching for the meaning of life.

После заголовка следует пустая строка, а за ней начинается тело сообщения в кодировке ASCII. Настоятельно рекомендуем вам самостоятельно послать почтовому серверу сообщение, содержащее несколько строк заголовка, включая строку Subject:. Для этого с помощью программы Telnet следует установить TCP-соединение с нужным сервером, введя следующую строку: telnet serverName 25

Теперь рассмотрим, что такое MIME-расширение для кодировки, отличной от ASCII. Если приведенные выше заголовки подходят для сообщений, содержащих текст в кодировке ASCII, то их содержимого недостаточно для сообщений с аудио-, видео- и прочей информацией, формат которой не соответствует ASCII. Это требует включения в сообщение специальных заголовков, а следовательно, расширения стандарта RFC 822. Такое расширение описано в документах RFC 2045 и 2046 и носит название многоцелевых расширений почты Интернета (Multipurpose Internet Mail Extensions, MIME).

Двумя наиболее важными MIME-заголовками, предназначенными для поддержки мультимедиа, являются Content-Type: и Content-Transfer-Encoding:. Заголовок Content-Type: позволяет агенту получателя произвести соответствующую обработку данных сообщения. Так, например, если сообщение содержит изображение в формате JPEG, агент получателя вызовет процедуру декомпрессии файлов JPEG. Для того чтобы понять смысл второго заголовка, Content-Transfer-Encoding:, вспомните о том, что все данные в кодировке, отличной от ASCII, перед передачей по протоколу SMTP должны быть преобразованы в кодировку ASCII.



Заголовок Content-Transfer-Encoding: указывает адресату на то, что было произведено преобразование (кодирование) исходной кодировки символов в кодировку ASCII, а также на тип этого кодирования. Таким образом, агент получателя, распознав заголовок Content-Transfer-Encoding:, сможет произвести декодирование сообщения для приведения данных в исходную кодировку, а затем, распознав заголовок Transfer-En- coding:, обработать декодированные данные.

Рассмотрим конкретный пример. Пусть Алиса хочет переслать Алексу электронное письмо, содержащее JPEG-изображение. Для этого она вызывает свой агент, вводит адрес почтового ящика Алекса, указывает тему сообщения и вставляет изображение в тело сообщения (в зависимости от используемого агента вставка файла может называться «присоединением»). После команды отправки агент генерирует MIME-сообщение, выглядящее так:

From: alice@crepes.fr
To: alex@hamburg.edu
Subject: Picture of yummy crepe.
MIME-Version: 1.0 Content-
Transfer-Encoding: base64
Content-Type: image/jpeg
(base64 encoded data
base64 encoded data)

Из приведенного сообщения можно узнать о том, что агент пользователя Алисы кодировал JPEG-изображение методом base64. Этот метод стандартизирован документом RFC 2045 как способ преобразования в 7-разрядную кодировку ASCII. Другим часто используемым методом кодирования является преобразование 8-разрядных данных в кодировке ASCII (обычно символов национальных алфавитов) в 7-разрядные.

Когда Алекс станет читать письмо Алисы, его агент сначала обнаружит строку Content- Transfer-Encoding: base64 заголовка и декодирует тело сообщения методом base64. Затем агент увидит строку Content-Type: image/jpeg и произведет JPEG-декомпрессию полученных данных. Строка MIME-Version: 1.0 идентифицирует номер версии MIME. При отсутствии этой строки сообщение будет обработано как стандартное, соответствующее формату RFC

822/SMTP. Как правило, заголовок сообщения отделяется от тела пустой строкой.

Рассмотрим подробнее строку Content-Type: заголовка. Согласно спецификации MIME, указанной в RFC 2046, формат строки имеет следующий вид:

Content-Type: type/subtype: parameters

Здесь parameters — это необязательные параметры. Согласно спецификации, строка Content-Type: используется для указания типа данных, передаваемых в сообщении, и состоит из имен типа и подтипа. Кроме того, в строке могут присутствовать параметры, предназначенные для уточненной информации о подтипе и не оказывающие значимого влияния на интерпретацию данных. Разумеется, для каждого подтипа определяется собственный набор параметров. Разработка MIME велась с расчетом на будущую расширяемость, и не исключено, что скоро число возможных пар типов и подтипов значительно возрастет. Для того чтобы как-то упорядочить разработку новых типов и подтипов, MIME предусматривает необходимость регистрации в IANA (Internet Assigned Numbers Authority — уполномоченная организация по назначению номеров Интернета). Регистрационный процесс описан в документе RFC 2048.

### 8.6.3. Протоколы доступа к электронной почте

После того как письмо Алисы попадает на почтовый сервер Алекса, оно помещается в почтовый ящик Алекса. Во всех предыдущих примерах мы неявно предполагали, что Алекс читает письма, входя на свой почтовый сервер и запуская программу чтения почты непосредственно на сервере. Действительно, до середины 1990г.г. XXв. такая схема доступа к электронным сообщениям была самой распространенной. В последние годы более типична ситуация, когда пользователь просматривает сообщения с помощью агента, выполняющегося на его вычислительной машине (офисном персональном компьютере, компьютере семейства Macintosh или цифровом органайзере). Это открывает пользователю доступ к набору удобных средств для работы с электронной почтой, в частности к средствам просмотра мультимедиа-сообщений и разнообразных вложений.



На практике используется компромиссный вариант: пользователь просматривает электронную почту с помощью агента, находящегося на его персональном компьютере, однако прием входящих сообщений осуществляется почтовым сервером общего пользования, на котором расположен почтовый ящик пользователя. Обычно почтовые ящики предоставляются Интернет-провайдерами.

Итак, пользователи обрабатывают электронные сообщения с помощью своих персональных компьютеров, используя почтовые серверы лишь для отправки и получения почты. Возникает вопрос: каким образом осуществляется взаимодействие между агентами пользователей и почтовыми серверами? Сначала рассмотрим, как письмо Алисы попадает на почтовый сервер Алекса. Однако протокол SMTP описывает передачу сообщений между почтовыми серверами, а агент пользователя Алисы не имеет прямого соединения с почтовым сервером Алекса. Сначала агент пользователя устанавливает SMTP-соединение с почтовым сервером Алисы и осуществляет передачу сообщения, а уже затем происходит соединение почтовых серверов Алисы и Алекса, о котором шла речь ранее. Возникает вопрос: зачем использовать промежуточную передачу? Первой важной причиной является то, что агент пользователя Алисы не располагает эффективным механизмом реагирования на отсутствие ответов от почтового сервера Алекса. Как вы помните, почтовый сервер Алисы предпринимает периодические попытки установления соединения с почтовым сервером Боба до тех пор, пока одна из попыток не окажется удачной. В документах RFC содержатся описания способов передачи сообщений между несколькими SMTP-серверами с помощью SMTP-команд.

Теперь остается рассмотреть, каким образом агент пользователя Алекса получает сообщения, находящиеся в его почтовом ящике. Вспомним о том, что SMTP является протоколом отправки, а операция извлечения и доставки сообщений, очевидно, требует применения протокола получения. Таким образом, мы приходим к необходимости создания специального протокола получения электронной почты, находящейся в почтовом ящике сервера. Существует несколько таких протоколов, наиболее распространенными из которых являются POP3 (Post Office Protocol Version 3 — протокол почтового отделения, версия 3), IMAP (Internet Mail Access Protocol — протокол доступа к почте Интернета) и HTTP.

На рис.8.20 представлена схема, иллюстрирующая использование различных протоколов в системе электронной почты Интернета[71]. Как мы видим, протокол SMTP передает сообщения между почтовыми серверами отправителя и получателя, а также между агентом отправителя и почтовым сервером отправителя. От почтового сервера получателя агенту получателя сообщения доставляются по протоколу POP3.

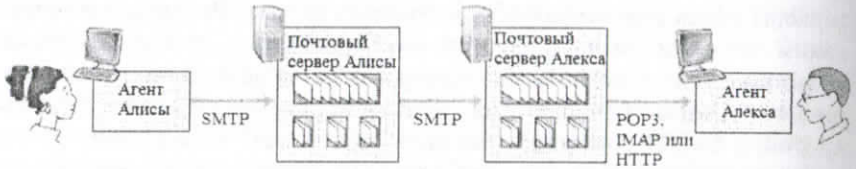



Рис.8.20. Протоколы электронной почты и их взаимосвязь

Протокол **POP3**, описанный в документе RFC 1939, является одним из самых простых протоколов доступа к электронной почте. Увы, простота протокола POP3 оборачивается его весьма ограниченной функциональностью. Протокол начинает действовать после того, как агент пользователя (клиент) устанавливает TCP-соединение с портом 110 почтового сервера, и подразумевает выполнение трех основных фаз: авторизации, транзакции и обновления. Во время авторизации агент передает серверу имя пользователя и пароль для того, чтобы сервер предоставил агенту доступ к сообщениям электронной почты. В фазе транзакции пользователь получает сообщения, а также может пометить сообщения, предназначенные для удаления, и получить почтовую статистику. Наконец, фаза обновления наступает после того, как клиент посылает команду quit и закрывает POP3-сеанс. Почтовый сервер производит удаление сообщений, помеченных пользователем. Во время POP3-транзакции агент пользователя посылает почтовому серверу команды, на каждую из которых сервер реагирует посылкой одного из двух ответных сообщений: +0K (иногда с последующей передачей данных сервера клиенту) и -ERR, указывающего на ошибку в команде клиента.

[71] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



Авторизация включает в себя две возможные команды: user <имя пользователя> и pass <пароль>.

Режим удаления переданных сервером сообщений имеет важный недостаток. Предположим, Алекс является мобильным пользователем и получает доступ к почтовому серверу с разных компьютеров (например, домашнего, офисного и портативного). Если каждый раз после передачи сообщений сервер будет удалять их, то часть сообщений окажется на персональном компьютере, часть — на офисном, а часть — на портативном. Таким образом, Алекс будет лишен возможности одновременного доступа ко всем полученным сообщениям. Если агенты пользователя на компьютерах Алекса будут настроены на загрузку сообщений без удаления, копии всех входящих сообщений останутся в почтовом ящике, что обеспечит доступ к ним с любого компьютера.

Хотя во время POP3-сеанса между почтовым сервером и агентом пользователя почтовый сервер сохраняет определенную информацию о состоянии (в основном это относится к списку сообщений, предназначенных для удаления), сохранять полную информацию о сеансе не нужно. Это в значительной степени упрощает реализацию почтового POP3-сервера.

Если Алекс использует протокол доступа к электронной почте POP3, он может создавать на своем компьютере специальные почтовые папки, в которые будут попадать загруженные с сервера сообщения. Кроме того, Алекс может удалять загруженные сообщения, перемещать их между папками и производить поиск сообщений по имени отправителя или теме. Такая система хранения сообщений, реализованная в виде папок на локальном компьютере, удобна для резидентного пользователя, однако вряд ли подходит в случае, если пользователь регулярно меняет вычислительные машины, с которых осуществляет доступ к электронной почте. Организация иерархии папок на почтовом сервере была бы весьма удобна для «мульти- компьютерных» пользователей. Именно по этой причине был разработан другой протокол доступа к почте – **IMAP**.

Протокол IMAP описан в документе RFC 2060. Он имеет много общего с протоколом POP3, однако его структура значительно сложнее; сложнее и реализация клиентской и серверной сторон **IMAP**.

IMAP-сервер связывает каждое сообщение с некоторой пользовательской папкой. Изначально каждое принятое сообщение

попадает в папку INBOX, где пользователь может прочитать его, а затем переместить в другую папку, удалить и т. п. Для всех подобных действий протоколом IMAP предусмотрены специальные команды. Удобной функцией является возможность поиска в каждой из папок писем, удовлетворяющих заданному критерию. Обратите внимание на то, что, в отличие от POP3, IMAP-сервер сохраняет информацию о ходе IMAP-сеанса, в том числе об именах папок, о том, какие сообщения в каких папках находятся, и т. п.

Еще одним важным достоинством IMAP является наличие команд, позволяющих пользователю получать отдельные компоненты сообщений: заголовки, части составных MIME-сообщений и т. д. Эта возможность удобна при низкоскоростных соединениях между пользователем и Интернет-провайдером. Некоторые пользователи предпочитают избегать загрузки длинных сообщений, содержащих несколько объемных вложений (например, аудио- или видеоклипов), и возможность выбирать нужные фрагменты для них весьма кстати. Более подробную информацию о протоколе IMAP вы можете получить на официальном сайте IMAP.

### 8.6.4. Электронная почта с web-интерфейсом

Все больше и больше пользователей Интернета получают доступ к своим электронным почтовым ящикам с помощью web-браузеров. Компания Hotmail первой применила web-технологии для работы с электронной почтой в середине прошлого десятилетия; в настоящее время эта услуга предлагается практически каждым порталом Интернета, а также большинством Интернет-провайдеров. При доступе к электронной почте через web-интерфейс роль агента пользователя играет web-браузер, который взаимодействует с удаленным почтовым ящиком по протоколу HTTP (см.рис.8.21). Когда Алекс хочет получить новые сообщения, он подключается к своему почтовому серверу, который отсылает Алексу сообщения по протоколу HTTP (а не SMTP или IMAP). Аналогично Алиса передает новые сообщения своему почтовому серверу через браузер по протоколу HTTP. Следует обратить внимание на то, что обмен сообщениями между почтовыми серверами Алисы и Алекса, как и ранее, происходит по протоколу SMTP (см.рис.8.22).



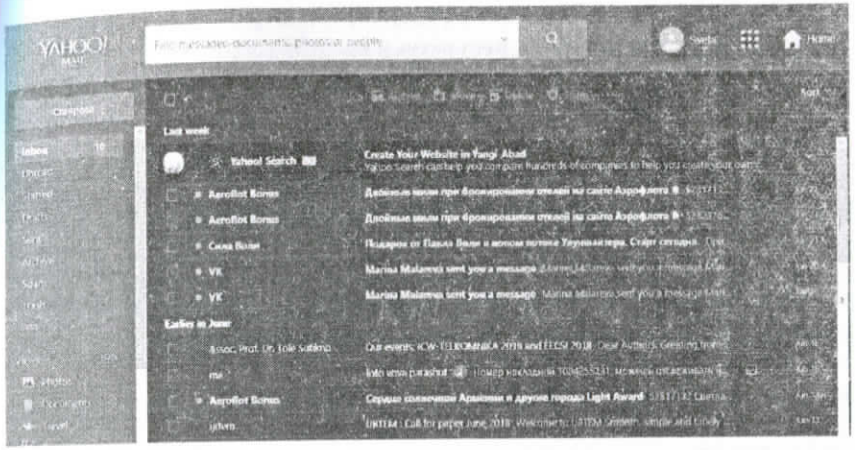



Рис.8.21. Пример доступа к почтовому ящику через web-интерфейс

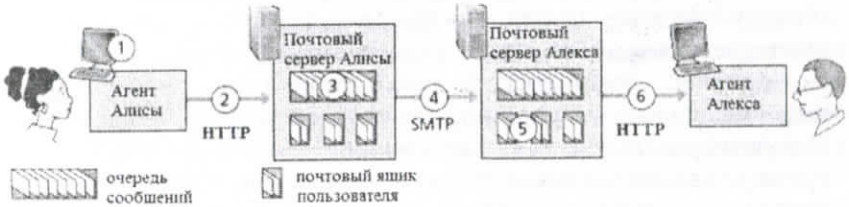



Рис.8.22. Взаимодействие протоколов электронной почты с web-интерфейсом

Механизм доступа к почте через web-интерфейс очень удобен для тех, кто регулярно пользуется несколькими компьютерами. Для чтения и отправки сообщений пользователю необходимо лишь иметь доступ к компьютеру или цифровому органайзеру с браузером, который может находиться дома, в офисе, в отеле, в Интернет-кафе. Как и в случае протокола IMAP, пользователи имеют возможность организовать иерархическую структуру папок в своем почтовом ящике; более того, для этого используются IMAP-серверы. Обычно доступ к папкам и сообщениям осуществляется с помощью скриптов, выполняющихся на HTTP-сервере; эти скрипты для доступа к IMAP-серверу используют протокол IMAP.

## 8.7. Сервис World Wide Web (WWW) – гипертекстовая система интеграции сетевых ресурсов в единое информационное пространство

### 8.7.1. Web и HTTP

До 1990г.г. XXв. пользователями ресурсов Интернета были исследователи, ученые и студенты, которые подключались к удаленным хостам, обменивались с ними файлами, получали сообщения из групп новостей и пользовались услугами электронной почты. Несмотря на то что Интернет-приложения уже тогда обладали огромной потенциальной пользой, Интернет еще был мало распространен среди широких масс. Ситуация резко изменилась в начале 1990-х годов с появлением Всемирной паутины (World Wide Web, WWW, или web). Без преувеличения можно сказать, что именно Всемирная паутина изменила взаимодействие между людьми, выделила Интернет из множества других компьютерных сетей (Prodigy, America Online, Compuserve, Minitel) и сделала слово «Интернет» синонимом термина «компьютерная сеть».

Главной особенностью web, отличающей ее от других информационных технологий, является ее активация **по запросу**. Пользователи получают ту информацию, которая им нужна, и в то время, когда она им нужна. Радио и телевидение, к примеру, лишены этой возможности, поскольку зрители и слушатели не имеют контроля над информационным потоком. Кроме того, в web механизм получения информации и ее размещения предельно прост. Каждый может за небольшую плату разместить в Сети массу сведений. Гиперссылки и поисковые системы позволяют не «утонуть» в океане разнообразных web-сайтов. Высококачественная графика увеличивает наглядность представляемой информации, а формы, скрипты, апплеты, элементы ActiveX и прочие средства позволяют сделать общение пользователя с сетью интерактивным. Web служит платформой для разработки новаторских продуктов, появившихся после 2003г., включая YouTube, Gmail и Facebook.

### 8.7.2. Обзор HTTP

В «сердце» web находится протокол передачи гипертекста (HTTP), являющийся протоколом прикладного уровня. Описание



HTTP можно найти в RFC 1945 и RFC 2616. Протокол HTTP реализуется с помощью двух программ: клиента и сервера, которые, находясь на разных оконечных системах, обмениваются HTTP-сообщениями. Порядок обмена и содержание сообщений описаны в протоколе. Перед тем как углубиться в изучение HTTP, сначала освоим терминологию, используемую в контексте web.

Каждая **web-страница**, или **документ**, состоит из **объектов**. Объект представляет собой обычный файл в формате HTML, изображение в формате JPEG или GIF, Java-апплет, аудиоклип и т. п., то есть единицу, обладающую собственным универсальным указателем ресурса (Uniform Resource Locator, URL). Как правило, web-страницы состоят из базового HTML-файла и объектов, на которые он ссылается. Так, если web-страница включает базовый HTML-файл и пять изображений, то она состоит из шести объектов. Ссылки на объекты, относящиеся к web-странице, представляют собой URL-адреса, включенные в базовый HTML-файл. URL состоит из двух частей: имени хоста сервера, на котором находится объект, и пути к объекту. Так, например, для URL www.someSchool.edu/someDepartment/picture.gif именем хоста является фрагмент www.someSchool.edu, а путем к объекту — фрагмент someDepartment/picture.gif. *Браузером* называется агент пользователя web; он отображает web-страницы, а также выполняет множество дополнительных служебных функций. Кроме того, браузеры представляют клиентскую сторону протокола HTTP. Таким образом, термины «браузер» и «клиент» в контексте web будут употребляться как эквивалентные.

**Web-сервер** содержит объекты, каждый из которых идентифицируется своим URL-адресом. Кроме того, web-серверы представляют серверную сторону протокола HTTP. К наиболее популярными web-серверам следует отнести Apache и Microsoft Internet Information Server.

Протокол HTTP определяет, каким образом клиенты запрашивают web-страницы, а серверы осуществляют передачу этих страниц. Основную идею о взаимодействии клиента и сервера можно понять из рис.8.23. Когда пользователь запрашивает web-страницу (например, совершает щелчок на гиперссылке), браузер посылает серверу HTTP-запрос объектов, составляющих web-страницу. Сервер получает запрос и высылает ответные сообщения, содержащие требуемые объекты.

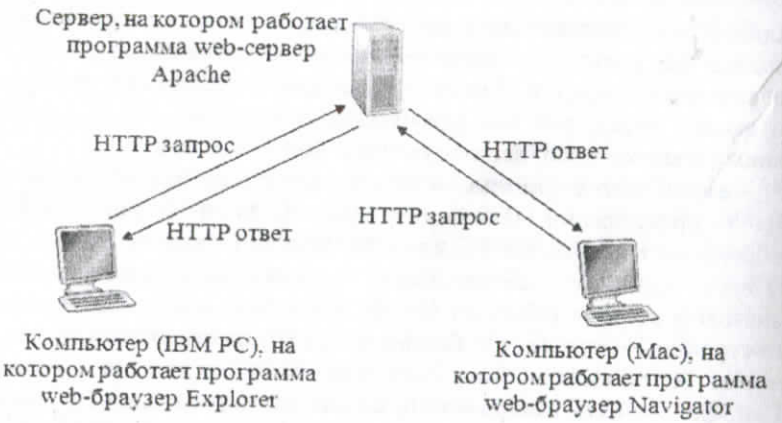



Рис.8.23. Передача запросов и ответов HTTP

Клиент посылает запросы и принимает ответы через свой интерфейс сокетов, а сервер использует интерфейс сокетов для получения запросов и их выполнения. После того как web-запрос минует сокет клиента, он оказывается «в руках» протокола TCP. Вспомним, что одной из функций протокола TCP является обеспечение надежной передачи данных; это означает, что каждый запрос, посылаемый клиентом, и каждый ответ сервера доставляются в виде, точно соответствующем отправленному. Здесь проявляется одно из достоинств многоуровневой коммуникационной модели: протоколу HTTP не нужно контролировать надежность передачи и обеспечивать повторную передачу пакетов при искажениях. Вся «черновая» работа будет проделана протоколом TCP и протоколами более низких уровней.

Необходимо отметить, что после завершения обслуживания клиентов сервер не сохраняет о них никакой информации. Если, например, какой-либо клиент сделает два запроса одного и того же ресурса подряд, сервер выполнит их, не выдав клиенту никакого оповещения о дублирующем запросе. Говорят, что протокол HTTP является **протоколом без запоминания состояния** (stateless protocol) соединения.



### 8.7.3. Постоянные и непостоянные соединения

Протокол HTTP поддерживает постоянные и непостоянные соединения. При непостоянном соединении протокол TCP получает лишь один объект, а при постоянном соединении — все объекты.

Для обсуждения механизма работы **непостоянного соединения** рассмотрим, каким образом осуществляется передача web-страницы от сервера к клиенту в случае непостоянного HTTP-соединения. Предположим, что страница состоит из базового HTML-файла и десяти JPEG-изображений, находящихся на одном сервере. Пусть URL базового HTML-файла имеет вид www.someSchool.edu/someDepartment/home.index. Процесс обмена между клиентом и сервером состоит из следующих шагов.

1. HTTP-клиент инициирует TCP-соединение с сервером www.someSchool.edu через порт номер 80, который по умолчанию является номером порта для HTTP.
2. HTTP-клиент посылает запрос серверу через сокет, выделенный TCP-соеди- нению, которое было установлено на шаге 1. Запрос включает путь к базовому HTML-файлу: someDepartment/home.index (чуть позже мы рассмотрим HTTP-сообщения более детально).
3. HTTP-сервер получает запрос через сокет, ассоциированный с установленным соединением, извлекает объект someDepartment/home.index, формирует ответ, включающий объект, и отсылает его клиенту через сокет.
4. HTTP-сервер закрывает TCP-соединение (окончательный разрыв соединения происходит после того, как сервер получает информацию об успешной передаче объекта).
5. HTTP-клиент принимает ответ сервера. TCP-соединение завершается. Клиент обрабатывает сообщение, в котором указано, что доставленный объект является базовым HTML-файлом. Клиент извлекает файл, обрабатывает его и выделяет ссылки на 10 объектов (JPEG-файлов).
6. Шаги 1-4 повторяются для каждого из 10 объектов.

После получения web-страницы браузер отображает ее на экране. Необходимо помнить, что различные браузеры могут по-разному интерпретировать одну и ту же web-страницу. Протокол HTTP никак не связан со способом визуализации web- страниц; спецификации, содержащиеся в документах RFC 1945 и RFC 2616,

описывают только метод обмена информацией между клиентом и сервером.

Теперь попробуем оценить величину временного интервала, проходящего с момента запроса клиентом web-страницы до окончания ее передачи. Здесь мы воспользуемся понятием **времени оборота** (Round-Trip Time, RTT), то есть времени, требующемуся пакету малой длины для передачи от клиента серверу и обратно. Время оборота включает в себя задержку распространения, ожидания и обработки. Рассмотрим, что происходит, когда пользователь совершает щелчок на гиперссылке. Как показано на рис.8.24, браузер инициирует TCP-соединение с web-сервером, которое устанавливается после «тройного рукопожатия»: клиент посылает серверу небольшой TCP-сегмент, сервер отвечает схожим сегментом (подтверждением), и наконец, клиент посылает серверу еще один сегмент-подтверждение. Для однократного обмена сегментами требуется время, равное времени оборота. Вместе с последним сегментом рукопожатия клиент отсылает серверу свой запрос, а сервер после получения запроса высылает клиенту базовый HTML-файл. Этот фрагмент взаимодействия также вызывает задержку на время оборота. Таким образом, суммарное время ответа складывается из удвоенного времени оборота и времени передачи базового HTML-файла.

Непостоянные соединения обладают рядом недостатков. Прежде всего для каждого запрашиваемого объекта должно устанавливаться новое соединение. При этом необходимо учитывать, что каждое соединение требует от протокола TCP выделения буфера, а также ряда служебных переменных как на стороне клиента, так и на стороне сервера. Учитывая то, что многие web-серверы параллельно обслуживают сотни клиентов, подобная схема серьезно затрудняет процесс взаимодействия между клиентами и сервером. Кроме того, установление соединения для каждого объекта из-за времени оборота приводит к дополнительным временным затратам.

При постоянном соединении сервер не закрывает TCP-соединение после обслуживания запроса, что позволяет обслужить несколько запросов в одном соединении.

Так, если в нашем примере применить механизм постоянных соединений, то вся web-страница, включающая базовый HTML-файл и 10 изображений, будет передана клиенту через одно TCP-соединение. Передача web-страниц через одно соединение возможна



в случаях, если все объекты находятся на одном и том же хосте. Обычно закрытие TCP-соединения происходит в случае, когда оно не используется в течение некоторого установленного времени (интервала ожидания).

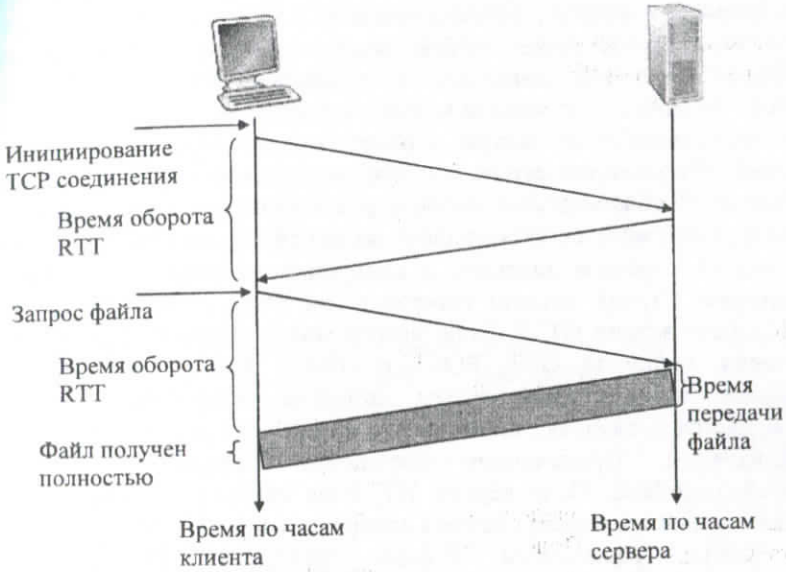



Рис.8.24. Оценка времени ответа на запрос HTML-файла

### 8.7.4. Формат HTTP-сообщений

Описания протокола HTTP, содержащиеся в документах RFC1945, RFC2616, определяют формат сообщений, предназначенных для обмена между клиентом и сервером. В HTTP существуют два типа сообщений: запросы и ответы, которые будут рассмотрены ниже.

Типичное **сообщение-запрос** протокола HTTP выглядит имеет вид:

```
GET /somedir/page.html HTTP/1.1
Host: www.someschool.edu
Connection: close User-agent:
Mozilla/5.0 Accept-language:fr
```

Это сообщение, несмотря на свою простоту, весьма наглядно демонстрирует формат, используемый в HTTP. Как можно видеть, Сообщение представляет собой совокупность вполне понятных человеку текстовых символов в кодировке ASCII. Сообщение состоит из пяти строк, каждая из которых оканчивается парой символов для перехода на новую строку (возврат каретки и перевод строки), а последняя строка — дополнительной парой указанных символов. В общем случае число строк сообщения может быть как больше, так и меньше пяти (вплоть до одной строки). Первая строка называется **строкой запроса**, а следующие строки — **строками заголовка**. Строка запроса содержит три поля: поле метода, поле URL и поле версии HTTP. Поле метода может принимать различные значения, например GET, POST и HEAD. Метод GET является наиболее часто используемым методом протокола HTTP и применяется в случаях, когда требуемый объект идентифицируется URL-адресом. Приведенное сообщение содержит URL-адрес /somedir/page.html. Поле версии HTTP не требует дополнительных комментариев и в нашем примере содержит запись HTTP/1.1.

Теперь рассмотрим строки заголовка. Строка Host: www.someschool.edu содержит адрес хоста, на котором находится объект. С помощью строки Connection: close браузер сообщает серверу о том, что не следует использовать постоянное соединение, и установленное TCP-соединение должно быть закрыто сразу после передачи требуемого объекта. Обратите внимание, что при этом браузер поддерживает версию 1.1 протокола HTTP. В строке The User-agent: указан агент пользователя, то есть тип браузера, сгенерировавшего запрос. В данном случае это браузер Mozilla 5.0 фирмы Netscape. Строка User-agent: является весьма полезной, поскольку на сервере могут храниться несколько версий одного документа, предназначенных для разных браузеров и адресуемых одним URL-адресом. Наконец, строка Accept- language: указывает на то, что пользователю по возможности должна быть выслана версия документа на французском языке (в случае ее наличия на сервере); в противном случае будет выслана версия документа на языке,



заданном по умолчанию. Строка Accept-language: является одной из множества заголовочных строк согласования данных, предусмотренных протоколом HTTP.

Рассмотрев конкретный пример, обратимся теперь к общему формату запроса (см.рис.8.25)[72]. Как можно видеть, пример вполне соответствует этому формату; тем не менее после строк заголовка и пустой строки формат сообщения предусматривает наличие тела сообщения. Тело сообщения остается пустым при использовании метода GET и заполняется при использовании метода POST. Метод POST применяется в случаях, когда пользователь заполняет формы, например вводит слово для поиска в поисковой системе. Заполнение форм приводит к генерации запроса, а содержимое web-страницы зависит от данных, введенных в формы. Итак, если поле метода содержит значение POST, то в теле сообщения находятся данные, введенные в формы.

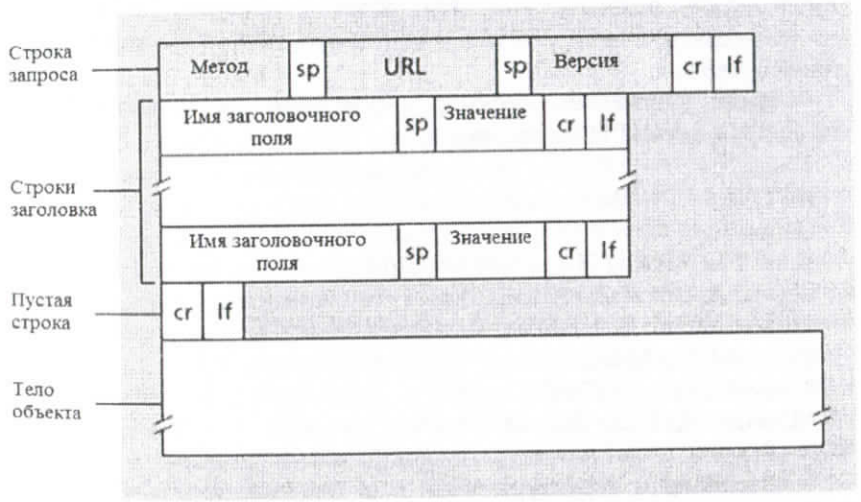



Рис.8.25. Общий формат сообщения-запроса

Необходимо отметить, что в запросах, создаваемых с помощью форм, не всегда применяется метод POST. Напротив, HTML-формы часто

[72] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

используют метод GET и подставляют введенные значения в URL-адрес требуемой страницы. К примеру, если пользователь ввел в формы два значения, monkeys и bananas, то запрашиваемый с помощью метода GET URL-адрес будет иметь вид www.somesite.com/ani- malsearch?monkeys&bananas. Вполне вероятно, что вы нередко встречали подобные конструкции, путешествуя в web.

Метод HEAD схож с методом GET. При получении запроса с методом HEAD сервер формирует ответ, однако не осуществляет пересылку объекта. Разработчики приложений часто используют метод HEAD для отладки ошибок.

В спецификации HTTP/1.0 указаны лишь три метода: GET, POST и HEAD. Спецификация HTTP/1.1 располагает более широким набором методов, в который, кроме перечисленных выше, входят PUT и DELETE. Метод PUT часто применяется в средствах web-публикаций и позволяет поместить объект с заданным URL- адресом на web-сервер, а метод DELETE — удалить объект, расположенный на web- сервере.

Ниже приведен пример типичного **сообщения-ответа**, генерируемого HTTP-сервером.

```
HTTP/1.1    200    OK
Connection: close
Date: Tue, 09 Aug 2011 15:44:04 GMT
Server: Apache/2.2.3 (CentOS)
Last-Modified: Tue, 09 Aug 2011 15:11:03 GMT
Content-Length: 6821
Content-Type: text/html
(data data data data data ...)
```

Рассмотрим структуру этого сообщения. Оно состоит из трех частей: **строки состояния**, шести **строк заголовка** и **тела сообщения**. Тело сообщения содержит требуемый объект. Строка состояния образована из трех полей: поля версии протокола, поля кода состояния и поля соответствующей коду информации, описывающей это состояние. В данном примере строка состояния говорит о том, что сервер использует спецификацию HTTP/1.1, требуемый объект найден и осуществляется его пересылка.



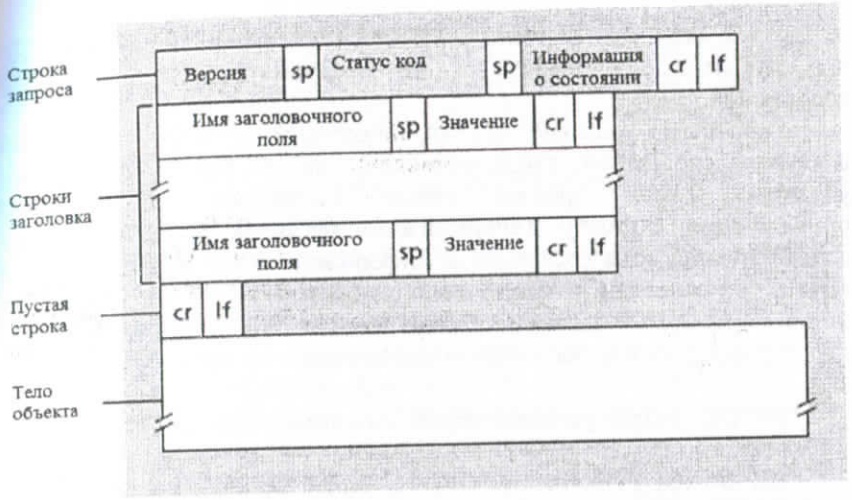



Рис. 8.26. Общий формат сообщения-ответа

Теперь обратимся к строкам заголовка. Сервер использует строку Connection: close для уведомления клиента о том, что TCP-соединение будет закрыто после того, как окончится пересылка объекта. Строка The Date: содержит дату и время создания ответа. Обратите внимание, что эта дата не относится к созданию или последнему изменению объекта, а указывает момент извлечения объекта из места его хранения и включения в тело сообщения. Строка Server: говорит о том, что сообщение было создано сервером Apache, и она аналогична строке User-agent: в сообщении-запросе. Строка Last-Modified: содержит дату и время создания или последнего изменения объекта. Как мы увидим немного позже, содержимое строки Last-Modified: крайне важно для кэширования объектов как на локальных клиентах, так и на сетевых кэш- серверах (часто называемых прокси-серверами). Строка Content-Length: содержит размер пересылаемого объекта в байтах, а строка Content-Type: указывает на то, что объект является текстом в формате HTML (обратите внимание, что тип объекта определяется содержимым строки Content-Type: и не зависит от расширения файла).

Если сервер получает запрос, в котором указана версия HTTP/1.0, постоянное соединение не будет использоваться, даже при

поддержке сервером протокола HTTP/1.1. Это необходимо потому, что спецификация HTTP 1.0 не предусматривает постоянных соединений.

Рассмотрев частный случай, обратимся к общему формату ответного сообщения, представленному на рис.8.26[73]. Как можно убедиться, наш пример также полностью соответствует приведенному формату. Теперь скажем несколько слов о том, что означают поля кода состояния и информации о состоянии. Эти два поля взаимосвязаны и фактически отражают результат обработки запроса. Ниже приведены несколько наиболее часто встречающихся пар, содержащих код состояния и информацию об этом состоянии.

200 OK: Запрос успешно обработан, объект получен и включен в ответ.
301 Moved Permanently: Объект был перемещен; новый URL-адрес указан в строке ответа Location: Программа клиента автоматически выполнит запрос по новому адресу.
400 Bad Request: Общая ошибка, вызванная невозможностью интерпретации запроса сервером.
404 Not Found: Запрашиваемый документ не найден на сервере.
505 HTTP Version Not Supported: Указанная в запросе версия HTTP не поддерживается сервером.

### 8.7.5. Взаимодействие пользователя с сервером – Cookie

Мы выяснили, что HTTP-сервер не запоминает информацию о состоянии соединения. Это упрощает разработку сервера и позволяет достичь значительной производительности за счет одновременного обслуживания сотен TCP-соединений. Тем не менее возможность распознавания пользователей сервером является весьма желательной. Причиной этому может служить необходимость разграничения прав доступа к информации, находящейся на сервере, либо предоставление каждому пользователю собственного набора информационных услуг. Для этих целей протокол HTTP использует объекты cookie.

Объекты cookie являются альтернативным авторизации

[73] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013



средством идентификации пользователей. Описание cookie находится в документе RFC 2109. Обычно объекты cookie находят применение в Интернет-порталах, электронной коммерции (например, Amazon) и рекламе (например, Double Click). Технология cookie подразумевает наличие четырех основных компонентов (см.рис.8.27)[74]:

- заголовочной cookie -строки в ответном сообщении сервера;
- заголовочной cookie -строки в запросе клиента;
- cookie-файла, находящегося на стороне клиента и обрабатываемого браузером;
- удаленной базы данных, расположенной на web-сайте.

Рассмотрим типичный пример использования объекта cookie. Предположим, пользователь применяет для доступа в web один и тот же браузер (пусть это будет Internet Explorer) и впервые оказывается на сайте Amazon.com, предоставляющем услуги электронной коммерции. Доступ к сайту осуществляется при помощи технологии cookie. При первом доступе сервер Amazon Web генерирует уникальный идентификационный номер для пользователя, создает в своей базе данных запись с индексом, равным идентификационному номеру, и отсылает клиенту пользователя ответное сообщение, включающее специальную строку Set-cookie: заголовка, содержащую идентификационный номер. Пример такой строки:

Set-cookie: 1678

Получив ответ, браузер анализирует его и добавляет строку Set-cookie: в cookie-файл. Этот файл содержит имена хостов и соответствующие идентификационные номера серверов. Каждый раз при формировании запроса к web-сайту браузер обращается к cookie-файлу, извлекает из него нужный идентификационный номер, включает его в запрос и отсылает серверу. В каждом таком запросе содержится строка заголовка вида:

cookie: 1678

Таким образом, сервер может собирать информацию о деятельности

[74] J.Kurose, K.Ross. Computer networking ATop-Down Approach. Sixth edition. Pearson Education, 2013

у себя пользователя: времени доступа, посещенных страницах и т. п. Это, в свою очередь, позволяет серверу организовать «карту покупателя» со списком сделанных во время сеанса покупок и дает возможность сразу оплатить их.

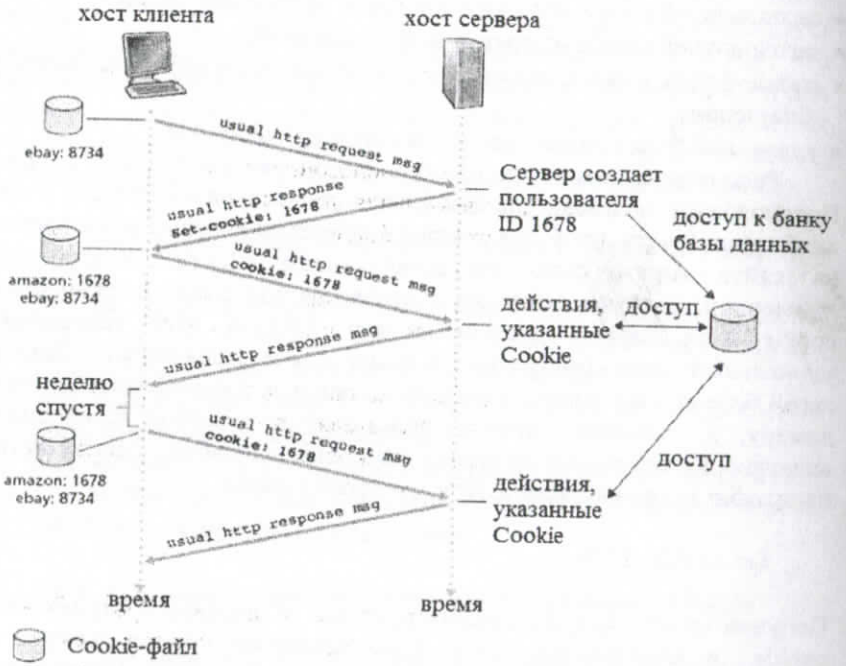



Рис.8.27. Идентификация пользователя с помощью cookie

При повторных входах на сайт идентификационный номер снова будет передан серверу. Сервер, располагающий информацией о предыдущих покупках пользователя, может на ее основе составить рекомендации о новых покупках. Зачастую подобные коммерческие сайты позволяют пользователям пройти регистрацию, указав свои имя, фамилию, почтовый адрес, номер кредитной карты, адрес электронного почтового ящика и др. Введенные данные заносятся в базу данных сервера. Именно с помощью описанного механизма осуществляется «покупка одним щелчком мыши» — потребность ввода личных данных отпадает.



Итак, объекты cookie представляют собой средство идентификации пользователей. При первом сеансе доступа пользователь вводит какой-либо идентификационный параметр (например, свое имя), а сервер в ответном сообщении отсылает пользователю заголовочную cookie-строку, идентифицируя его. Кроме того, технология cookie позволяет создать подобие дополнительного «сеансового уровня» для протокола HTTP, не запоминающего информацию о соединении. К примеру, когда пользователь подключается к web-приложению электронной почты, браузер отсылает cookie-информацию серверу, позволяющую идентифицировать пользователя во время сеанса.

Несмотря на то что объекты cookie позволяют упростить процесс покупок для пользователя, они, как и приведенная выше схема авторизации, весьма ненадежны с точки зрения обеспечения конфиденциальности информации. Как мы убедились, процедура регистрации приводит к выдаче пользователем данных личного характера, которые при использовании небезопасного cookie-доступа могут стать известны другим людям. Кроме того, объекты cookie могут применяться для сбора информации о поведении пользователя на множестве web-сайтов.

## 8.8. Сервис SE – поисковые системы

### 8.8.1. Назначение сервиса SE

Сервис SE (Search Engine) – поисковые системы – это специальные Web-сайты, на которых пользователь по заданному запросу может получить ссылки на сайты, соответствующие этому запросу. Установлено, что 85% пользователей Интернет используют поисковые системы, чтобы найти необходимые им товары, услуги и информацию.

Поисковые системы отличаются от тематических каталогов. Они представляют собой серверы с огромной базой URL-адресов, которые автоматически обращаются к Web-страницам по этим адресам, изучают содержимое этих страниц, формируют и прописывают ключевые слова со страниц (индексируют страницы). Более того, эти серверы обращаются по всем встречаемым на страницах ссылкам и, переходя к новым страницам, проделывают с ними то же самое. Так как почти любая Web-страница имеет

множество ссылок на другие страницы, то при подобной работе поисковая система в конечном результате теоретически может обойти все сайты в Internet.

Поисковая система состоит из следующих основных компонентов:

1. Паук (spider) – программа, которая скачивает Web-страницы тем же способом, что и браузер пользователя. Отличие состоит в том, что браузер отображает информацию, содержащуюся на странице (текстовую, графическую и т. д.), паук же не имеет никаких визуальных компонент и работает напрямую с html-текстом страницы (можно сделать «просмотр html-кода» в браузере, чтобы увидеть
2. Путешествующий паук (crawler) – программа, которая выделяет все ссылки, присутствующие на странице. Ее задача – определить, куда дальше должен идти паук, основываясь на ссылках или исходя из заранее заданного списка адресов. Краулер, следуя по найденным ссылкам, осуществляет поиск новых документов, еще неизвестных поисковой системе.
3. Индексатор (indexer) – программа, которая разбирает страницу на составные части и анализирует их. Выделяются и анализируются различные элементы страницы, такие как текст, заголовки, структурные и стилевые особенности, специальные служебные html-теги и т. д. Результатом анализа является index-файл.
4. База данных (database) – это хранилище всех index-файлов, полученных поисковой системой в процессе скачивания и анализа Web-страницы. Иногда базу данных называют индексом поисковой системы.
5. Система выдачи результатов (search engine results engine) – занимается ранжированием страниц. Она решает, какие страницы удовлетворяют запросу пользователя, и в каком порядке они должны быть отсортированы. Это происходит согласно алгоритмам ранжирования поисковой системы. С этим компонентом поисковой системы взаимодействует оптимизатор, пытаясь улучшить позиции сайта в выдаче с помощью определенных факторов, влияющих на ранжирование результатов.
6. Web-сервер (Web – server) – сервер, который осуществляет взаимодействие между пользователем и остальными компонентами поисковой системы. Как правило, на сервере



присутствует html-страница с полем ввода, в котором пользователь может задать интересующий его поисковый термин. Web-сервер также отвечает за выдачу результатов пользователю в виде html-страницы.

Детальная реализация поисковых механизмов может отличаться друг от друга. Например, связка spider+crawler+indexer может быть выполнена в виде единой программы, которую называют поисковым роботом. Она скачивает известные Web-страницы, анализирует их, ищет по ссылкам новые ресурсы, индексирует их и заносит в базу данных в виде index-файла. Поиск осуществляется другой программой, которая извлекает запрашиваемую пользователем информацию из index-файла. Однако всем поисковым системам присущи описанные общие черты.

### 8.8.2. Критерии ранжирования документов

В поисковых системах ссылки на документы сортируются (ранжируются) по мере соответствия запросу. Для ранжирования страниц в поисковой выдаче используются текстовые критерии, ссылочные критерии и критерии пользовательской оценки.

Текстовые критерии определяют релевантность документа по совпадению слов и их сочетаний в запросе и тексте и заголовке страницы.

Релевантность документа – показатель, отражающий соответствие содержания документа конкретному запросу поисковой системы. Поисковые системы рассчитывают релевантность документа, строя частотный ряд из встречающихся на странице слов и словосочетаний. Чем чаще они встречаются в документе, тем большую по отношению к запросу пользователя релевантность он получает.

Поисковые системы отображают ссылки на Web-страницы документов в порядке убывания релевантности частями по 10 – 20 ссылок. Согласно данным маркетинговых исследований около 60% пользователей ограничиваются первой страницей результатов поиска и почти 90% – первыми тремя страницами. Отсюда следует задача для специалистов по сайтпромоутингу – добиться, чтобы независимо от построения запроса страницы Web-сайта стояли в первых 10-20 результатах поиска.

Основные текстовые критерии ранжирования документов приведены в табл. 8.2.

Таблица 8.2.

Текстовые критерии ранжирования документов

| Критерии | Логика ранжирования |
|---|---|
| «Вес» слова | Чем выше частота повторения слова в документе, тем больше ранг документа |
| Взаимное положение слов | Учет полного совпадения фраз или их подобия (например, порядок и близость слов друг к другу) |
| Положение найденного текста по отношению к началу документа | Считается, что чем ближе расположена информация к началу документа, тем выше ее значение |
| Наличие слов запроса в выделенных фрагментах и заголовках | Значимость обнаружения искомого текста в выделенных фрагментах считается выше, чем в обычном тексте |
| Совпадение темы страницы с темой запроса | Использование в поиске слов, не содержащихся в тексте запроса, но соответствующих теме запроса |
| Совпадение названия домена или файла с ключе вым словом | Поисковые машины придают дополнительный «вес» страницам, у которых домен или имя файла совпадают с ключевым словом |
| Совпадение поискового запроса с описанием из каталога | Сайт получает более высокий рейтинг, если слова поискового запроса совпадают с описанием каталога поисковой системы |
| Значимость редких слов | Значимость каждого из поисковых слов тем больше, чем реже оно встречается в документе |

Оценку значимости фрагментов текста выработал Г.Лун. Он предложил оценивать фрагменты текста по следующему выражению:



$$V = \frac{N_k^2}{N_0}$$

где: V – значимость фрагмента; $N_k$ – число ключевых слов в данном фрагменте; $N_0$ – общее число слов во фрагменте.

Система выявления ключевых слов обычно использует статистический частотный анализ (методика В. Пурто). Пусть:

F – частота, с которой встречаются различные слова в тексте;

P – относительное значение полезности (важности);

C – константа, которая определяет соотношение частоты слов и их полезности.

Тогда зависимость F (P) определяется формулой:

$$F(P) = C\frac{1}{P}$$

Данное положение предполагает существование двух граничных значений частот:

- слова с частотой менее нижней границы считаются слишком редкими (не способными отразить смысл документа), а с частотой , превосходящей верхнюю границу, считаются общими, не несущими смысловой нагрузки;
- слова с частотой, находящейся между этими границами, в наибольшей степени характеризуют содержимое данного конкретного документа.

Согласно ссылочным критериям, документ ранжируется с учетом индекса цитирования.

Индекс цитирования – это показатель известности сайта в Интернете, определяемый числом и значимостью ссылок на других сайтах на искомый ресурс. Общее число внешних ссылок на сайт не подходит в качестве критерия для расчета цитируемости, т. к. значимость ссылок на непопулярных ресурсах ничтожна по сравнению со значимостью ссылок с известных сайтов.

При определении индекса цитирования учитывается не только число внешних ссылок на сайт, но индекс цитирования самих сайтов, ссылающихся на данный. Наиболее ценные ссылки – ссылки, размещенные на головной странице высокоцитируемых сайтов. В общем случае каждая прямая ссылка на Web-страницу увеличивает ее цитируемость на величину, пропорциональную цитируемости

ссылающейся страницы и обратно пропорциональную общему числу ссылок на ссылающейся странице.

В свое время двумя американскими аспирантами Сергеем Брином и Ларри Пейджем, основавшими в 1997г. поисковую машину Google, была разработана модель, эмулирующая движение пользователя по документам в сети. При этом предполагалось, что пользователь с равной долей вероятности перейдет по любой из ссылок, содержащихся в документе, который он в данный момент просматривает. Следовательно, вероятность пользователя попасть на конкретный документ зависит от количества ссылок на него с других документов и от того, насколько вероятно нахождение пользователя на одном из ссылающихся документов и сколько исходящих ссылок содержит этот документ. Эта вероятность и была принята за показатель авторитетности или ранг страницы (PageRank):

$$PR_a = (1-d) + d \sum_{i=1}^{n} \frac{PR_i}{C_i},$$

где: $PR\ a$ – PageRank страницы $a$; $d$ – коэффициент затухания (означает вероятность того, что пользователь, зашедший на страницу, перейдет по одной из ссылок, содержащейся на этой странице, а не прекратит путешествие по сети), обычно устанавливают равным *0,85*; $i$ – страница, содержащая ссылки на страницу $a$ ($i$ изменяется от 1 до n); $PR\ i$ PageRank страницы $i$, ссылающейся на страницу $a$; $C_i$ общее число ссылок на странице $i$; $1 / C\ i$ - вероятность того, что пользователь, находящийся на странице $i$; из $C\ i$ доступных ему ссылок выберет именно ссылку на страницу страницу $a$; $d*PR_i\ C_i$ поток «теоретической посещаемости», который дойдет до страницы $a$ со страницы $i$ (суммирование идет по всем страницам, ссылающимся на страницу $a$); $(1 - d)$ минимальный PageRank страницы (он не равен нулю за счет того, что пользователь регулярно выбирает новый сайт в качестве стартовой точки).

Одним из распространенных заблуждение является то, что можно вычислить PageRank по этой формуле для отдельно взятого документа, используя известные значения PageRank для ссылающихся на него документов. Так делать нельзя. Чтобы вычислить PageRank какого-либо документа, надо составить систему



N линейных уравнений данного вида для каждого из документа из поисковой базы, где N – количество документов в поисковой базе. Причем, для выполнения условия, что сумма значений PageRank для всех документов (т. е. вероятность того, что пользователь находится на любой из страниц) равна 1, к свободный члену (1 – d) в каждом уравнении добавляют множитель 1/N. Эта система будет содержать N неизвестных. Решив ее, получим значения PageRank для каждого документа, известного поисковой машине.

В поисковой базе крупнейших поисковых машин содержится огромное количество документов. Несмотря на то что матрица, соответствующая системе уравнений будет сильно разрежена численное решение этой системы требует огромных вычислительных мощностей. Поэтому поисковая система должна постараться максимально упростить процесс расчета, вводя некоторые допущения. Вот эти конкретные особенности реализации классической формулы PageRank, увы, составляют коммерческую тайну поисковых машин.

Согласно критерию пользовательской оценки для ранжирования страниц в поисковой выдаче используются системы оценки качества страниц пользователями, которые основаны на предположении: если пользователь переходит по ссылке, значит, он счел ее интересной, и если долго не возвращается на страницу поисковой системы, значит его ожидания подтвердились.

Поисковая система Rambler при ранжировании результатов поиска в ответах на поисковый запрос использует коэффициент популярности, определяемый числом пользователей, которые просматривали данную страницу за последние несколько недель. Данный коэффициент, как и алгоритм PageRank, основан на учете гиперссылок между страницами сети, однако эта реализация дополнительно использует данные о реальной посещаемости страниц, полученные от счетчика Top100. Дело в том, что «классические» ссылочные алгоритмы фактически учитывают мнение только одной категории пользователей сети – Web-мастеров. Действительно, если большому количеству Web-мастеров нравится тот или иной ресурс, они размещают на него ссылки. Обычные пользователи, как правило, созданием страниц и сайтов не занимаются, и поэтому учесть их мнение оказывается невозможно. Счетчик Top100 как раз и предназначен для того, чтобы сделать коэффициент популярности более справедливым.

Однако, судя по всему, в последнее время данные о посещаемости документов, полученные от счетчика Top100, оказывают все меньшее и меньшее влияние на коэффициент популярности, так как счетчик не в состоянии противостоять массовым накруткам, практикуемым владельцами некоторых сайтов. Соответственно, все большее значение приобретает составляющая, вычисляемая на основе учета гиперссылок между страницами сети.

В соответствии с изложенными критериями формулу, приближенно описывающую процесс определения релевантности документа запросу, можно представить следующим образом:

$$R_a(x) = \left(m * T_a(x) + p * L_a(x)\right) * F(PR_a)$$

где: $R_a(x)$ – итоговое соответствие документа $a$ запросу $x$; $T_a(x)$ – релевантность текста (кода) документа $a$ запросу $x$; $L_a(x)$ – релевантность текста с учетом ссылок с других документов на документ $a$ запросу $x$; $PR_a$ PageRank страницы a ; F ($PR_a$ ) монотонно неубывающая функция, причем $F(0) = 1$ и можно допустить, что $F(PR_a) = (1 + q * PR_a)$; $m$, $p$, $q$– весовые коэффициенты, определяемые разработчиком поисковой системы.

Резюмируя вышеизложенное, можно отметить, что для повышения ранга страницы необходимо работать над тем, чтобы как можно большее количество документов сети ссылалось на нее. Делать это можно различными способами – с помощью обмена ссылками с другими сайтами, регистраций в каталогах и различных тематических ресурсах и т. д. Идеальный способ – сделать свой сайт настолько уникальным и интересным, чтобы владельцы других ресурсов сами считали необходимым поставить ссылку на него. Не следует также забывать, что при расчете ранга документа учитываются как внешние, так и внутренние ссылки. Поэтому грамотная перелинковка документов внутри сайта позволяет повысить ранг самых важных из них с точки зрения содержащейся информации. Наиболее важные в этом смысле документы обязательно должны иметь ссылку с главной страницы сайта, которая, как правило, имеет максимальный ранг среди всех страниц сайта вследствие того, что на нее указывает большинство внешних ссылок на сайт.



### 8.8.3. Основные поисковые системы

В настоящее время существует три основных международных поисковых системы: Google, Yahoo и MSN Search, имеющих собственные базы и алгоритмы поиска. Большинство остальных поисковых систем использует в том или ином виде результаты 3-х перечисленных. Например, поиск AOL (search.aol.com) и Mail.ru используют базу Google, а AltaVista, Lycos и AllTheWeb – базу Yahoo.

В зоне русскоязычного Internet действуют более трех десятков поисковых систем. Причем около 90% аудитории используют 3 самые популярные поисковые системы: Яndex, Google, Rambler (табл.8.3).

Для поиска необходимых документов следует обратиться к конкретной поисковой системе и составить поисковый запрос, который может включать в себя одно или несколько слов. В запросе могут присутствовать знаки препинания. Составлять простые запросы можно и не вдаваясь в тон- кости языка запросов. Так, если ввести в поисковую строку несколько слов без знаков препинания и логических операторов, то будут найдены документы, содержащие все эти слова (причем на ограниченном расстоянии друг от друга). Однако знание и правильное применение языка запросов поисковой системы поможет сделать поиск быстрым и эффективным.

Таблица 8.3.

Поисковые системы русскоязычного Internet

| Поисковая система | Сервер | Доля аудитории |
|---|---|---|
| Яndex | http://www.yandex.ru | до 67 % |
| Google | http://www.google.co | до 33 % |
| Rambler | http://search.rambler.ru | до 20 % |
| Поиск@Mail.ru | http://go.mail.ru | до 15 % |
| АПОРТ | http://www.aport.ru | до 10 % |
| MSN | http://search.msn.com | до 3 % |
| Nigma | http://nigma.ru/ | до 3 % |
| Yahoo! | http://search.yahoo.co | менее 1 % |
| Altavista | http://www.altavista.co | менее 1 % |
| WebAlta | http://webalta.ru/ | менее 1 % |

Все поисковые системы используют сходные принципы языка запросов. Ссылку на полное описание языка запросов для каждой поисковой системы можно найти на ее главной странице. В большинстве языков запросов кроме простого запроса можно задавать операторы И (AND), ИЛИ (OR), НЕ (NOT), метасимвол *, заменяющий до 5 произвольных символов, коэффициентные символы + и –, служащие для увеличение или уменьшения значимости вводимых в запросе слов.

### 8.8.4. Поисковая система Яndex

Доступ к поисковой системе Яndex **(http://www.yandex.ru)** был открыт в 1997г. Поиск осуществляется не только по Web-страницам, но и по специализированным массивам данных, среди которых новости ведущих информационных агентств, товары Internet-магазинов, ресурсы WAP –серверов.

Яndex поддерживает собственный каталог Internet-ресурсов, формирующийся на основе индекса цитирования Яndex'a (CY – Citation Yandex). CY какой-либо Web-страницы измеряется количеством других страниц, содержащих ссылки на эту страницу. Этот метод оценки ресурсов принципиально отличается от простого учета количества посещений страницы.

Яndex имеет простой и расширенный поисковые интерфейсы, а также страницу настройки формата выдачи результатов поиска. Он использует собственную систему обозначений логических операторов, а также поддерживает большое количество поисковых функций.

В верхней части домашней страницы поисковой системы Яndex расположено поле для ввода ключевых слов (рис.8.31).

По умолчанию слова запроса связываются оператором OR. Под поисковым полем приводится пример формулировки запроса, меняющийся при каждом новом открытии страницы простого поиска. Селекторные кнопки снизу позволяют ограничивать поиск следующими областями: «Новости», «Маркет», «Карты», «Словари», «Блоги», «Картинки».

Поиск ключевых слов производится с учетом их морфологии. Если необходимо осуществить поиск по точной словоформе, то перед ним ставится знак «!» без пробела. Система различает слова, набранные строчными и прописными буквами. Поддерживается поиск по фразе, которая заключается в кавычки.



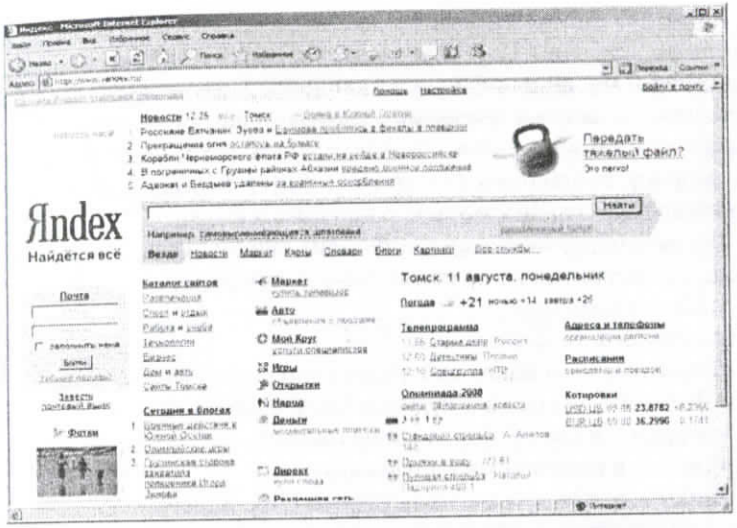



Рис.8.31. Домашняя страница поисковой системы Яndex

Перед ключевым словом допускается постановка знаков «+» и «–», которые заменяют логические операторы AND и NOT соответственно.

Яndex использует собственную систему обозначений логических операторов, которая одновременно позволяет задавать степень близости между ключевыми словами. Логические операторы AND и NOT обозначаются символами «&» и «~» соответственно. Употребление этих символов определяет наличие или отсутствие ключевых слов в отдельном предложении документа.

Для того чтобы подняться от уровня предложения до уровня всего документа, необходимо удвоить символ-оператор. Например, по запросу библиотеки && архивы будут найдены документы, содержащие оба слова без учета расстояния между ними, а по запросу библиотеки & архивы – документы, содержащие оба слова в пределах одного предложения.

Логический оператор OR вводится с помощью символа «|» и действует в пределах всего текста документа. Возможно также употребление круглых скобок для составления сложных поисковых предписаний.

Символ «/» ограничивает максимальное расстояние между ключевыми словами определенным числом. Например, по запросу библиотеки /5 архивы будут найдены документы, в которых расстояние между ключевыми словами не превышает 5 слов. Комбинация символов «/+» позволяет задать расстояние более точно. Так, запросу библиотеки /+2 архивы будут релевантны документы, содержащие фразу «библиотеки, областные архивы».

Также поддерживаются следующие специальные операторы для поиска в определенных областях html-документов:

**$title** – в заголовке;

**$anchor** – в тексте ссылок;

**#keywords=** – в ключевых словах (поле «keywords»);

**#abstract=** – поиск в описании (поле «META»);

**#image=** – в имени файла изображения;

**#hint=** – в подписи к изображению;

**#link=** – поиск ссылок на заданный URL-адрес;

**#url=** – поиск документов на заданном сайте (странице).

Интерфейс расширенного поиска системы Яndex представляет собой шаблон, состоящий из поля для ввода ключевых слов, их характеристик по месту расположения и употребления, а также свойств найденных страниц, различающихся по языку, дате и формату (рис.8.32).

Результаты поиска выдаются в виде заголовка документа, его описания, URL-адреса, а также ссылок на рубрику каталога Internet-ресурсов List.ru , в которую попадает данный документ (рис.8.33).

Результаты поиска сортируются по степени релевантности документов запросу и выдаются по 10 документов на страницу (рис.8.34).

Релевантность документа зависит от ряда факторов, в том числе от частотных характеристик ключевых слов, их близости в тексте документа, а также от веса слова – параметра, который пользователь может задать самостоятельно. Для этого используется символ «:» и определенное число. Например, по запросу «городские архивы» библиотеки: 3 будут найдены документы, содержащие фразу «городские архивы» и слово «библиотеки», но чем чаще в документе встречается слово «библиотеки», тем ближе он окажется к началу списка результатов.



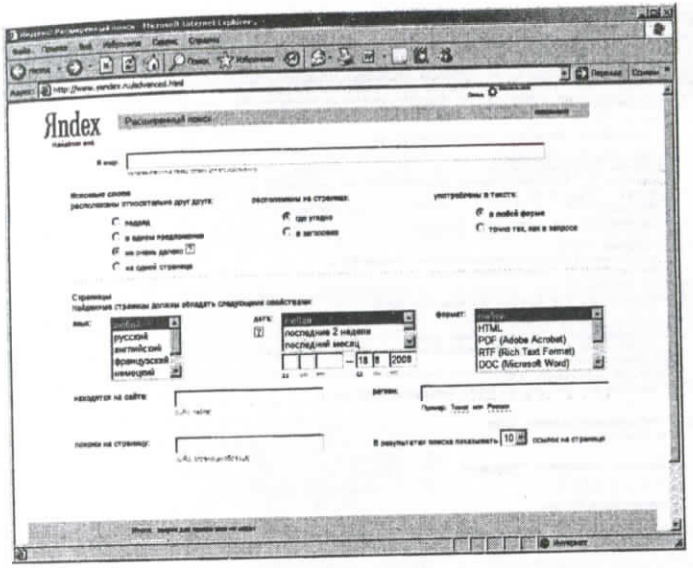



Рис.8.32. Интерфейс расширенного поиска системы Яndex

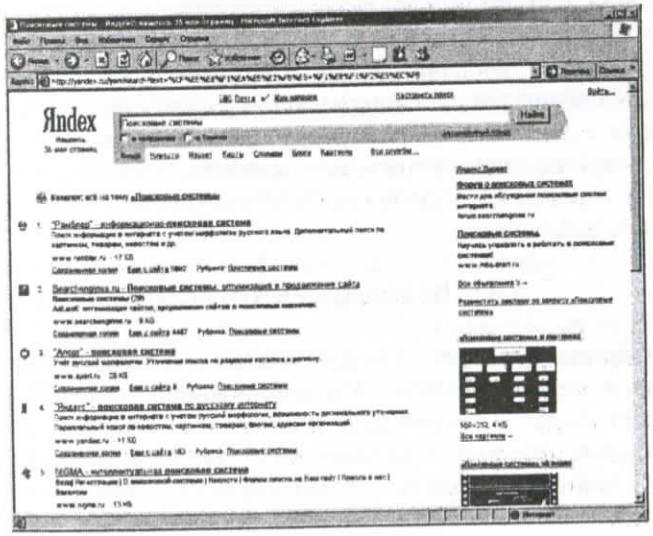



Рис.8.33. Результаты поиска системы Яndex

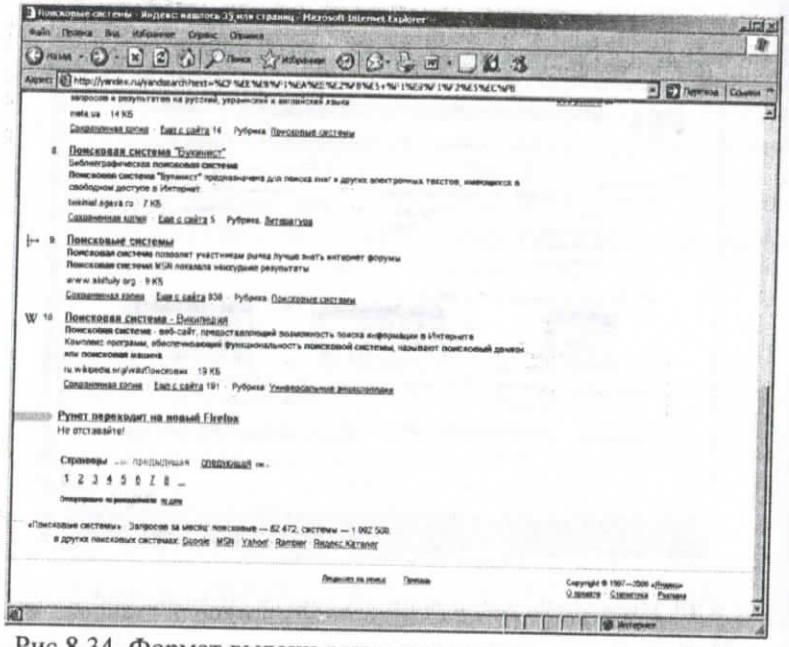


Рис.8.34. Формат выдачи результатов поиска системы Яndex

В числе дополнительных возможностей, предлагаемых пользователям поисковой системы Яndex, можно назвать следующие: интеграция с каталогом Internet-ресурсов List.ru, поиск по новостным лентам ведущих информационных агентств, поиск в электронных магазинах и поиск по российским WAP-ресурсам, а также программа «Региональный Яndex».

### 8.8.5. Поисковая система Google

Поисковая система Google **(http://www.google.com)** была открыта в сентябре 1999г. На сегодняшний день объем базы составляет более 1 миллиарда документов. Система предлагает пользователю простой и расширенный поисковый интерфейсы, а также страницу создания предустановок поиска (рис.8.35). Отличительной особенностью Google является технология определения степени релевантности документа путем анализа ссылок других источников на данный ресурс. Эта технология



называется PageRankTM. Чем больше ссылок на какую-либо Web-страницу имеется на других страницах, тем выше ее рейтинг в базе Google. При выдаче результатов поиска в начале списка оказываются страницы с более высоким рейтингом (при прочих равных составляющих).

Помимо основной базы запрос обрабатывается с использованием таких информационных массивов как БД RealNames и каталог Internet- ресурсов Google Web Directory.

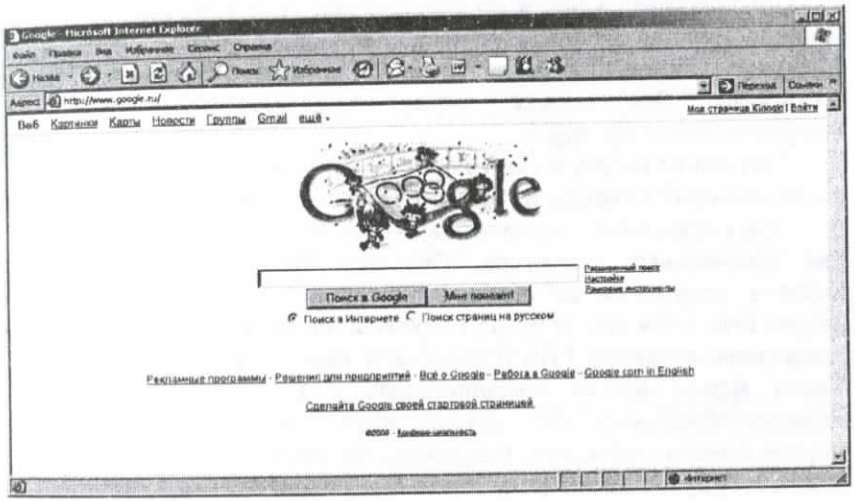


Рис.8.35. Домашняя страница поисковой системы Google

Google предоставляет доступ к своей базе другим поисковым системам, среди которых наиболее известными являются Netscape's Search и Yahoo!.

Основными достоинствами системы являются значительный объем базы, маленький список стоп-слов и возможность получения копии документа из базы Google, если он удален с основного адреса.

Поисковая система Google позволяет осуществлять *простой и расширенный поиски.* При обработке запроса система интерпретирует пробел между словами как логический оператор AND, однако ввод самого оператора не поддерживает. Запрос вводится в поисковое

поле. Справа расположены ссылки на страницу «Расширенный поиск» и страницы создания предустановок поиска: «Настройки» и «Языковые инструменты».

Если необходимо провести поиск с использованием стоп-слов, то перед ними проставляется знак «+». Система поддерживает использование логического оператора OR. Оператор NOT заменяется знаком «–» перед словом без пробела. Возможна постановка знаков «+» и «–» перед фразой.

Поддерживается поиск по фразе. Фраза заключается в кавычки. Помимо кавычек Google учитывает следующие знаки препинания, служащие для связи слов: дефисы, косые черты, знаки равенства, апострофы. При поиске слова, связанные этими знаками, воспринимаются как фраза.

Система не поддерживает поиск с учетом морфологии, поиск по части ключевого слова и не различает строчные и прописные буквы.

При составлении поискового выражения можно использовать два специальных оператора. Оператор link: дает возможность выявить документы со ссылкой на данный URL. Например, на запрос link: www. nlr. ru будут получены документы со ссылками на домашнюю страницу РНБ (Российской национальной библиотеки). Такой запрос нельзя комбинировать с обычными ключевыми словами. Оператор site: сужает круг поиска документами с определенного web-сайта. Например, по запросу site: www. nlr. ru database будут найдены документы на Web-сайте РНБ, содержащие слово «database».

Интерфейс страницы расширенного поиска реализован в виде шаблона, состоящего из фильтров (рис.8.36).

Поисковая система Google определяет степень релевантности документа путем анализа ссылок других источников на данный ресурс. При сортировке результатов поиска из всех релевантных документов выбираются страницы с более высоким рейтингом и помещаются в начало списка.

Перед списком результатов указывается количество документов, найденных по запросу, и время обработки запроса в базе Google (рис.8.37).

Формат вывода результатов поиска состоит из следующих элементов (рис.8.38):

- заголовок документа;



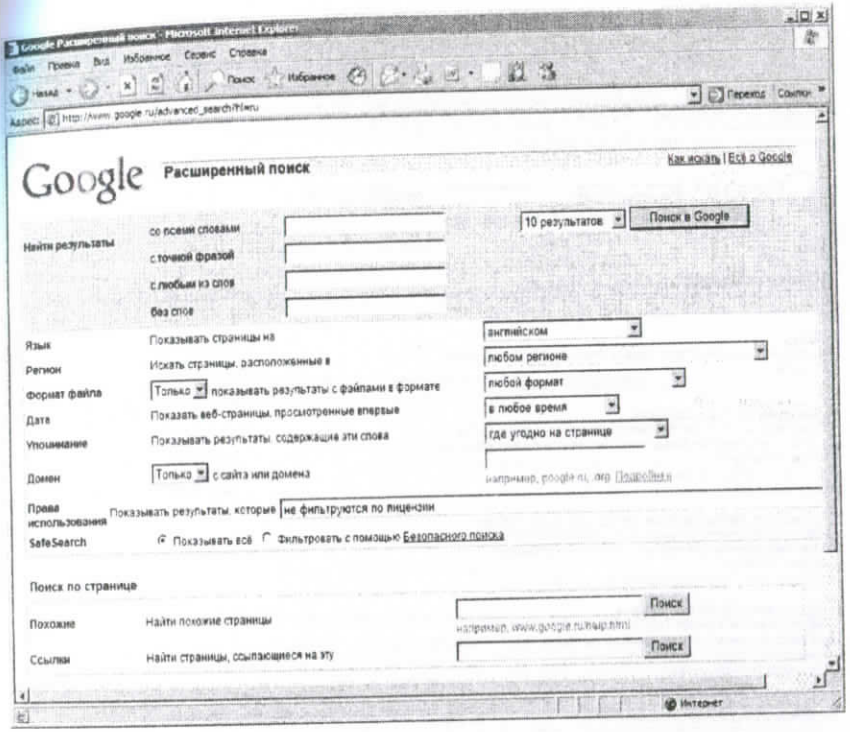



Рис.8.36. Интерфейс расширенного поиска системы Google

- выдержки из текста с выделенными жирным шрифтом словами запроса;
- описание документа, полученное из поля meta;
- ссылка на соответствующий раздел каталога Google Web Directory;
- URL-адрес страницы;
- размер найденного документа в килобайтах;
- ссылка на копию документа в базе Google;
- ссылка для задания поиска документов, наиболее релевантных дан- ному;
- другие страницы сайта, релевантные запросу, если таковые имеются.

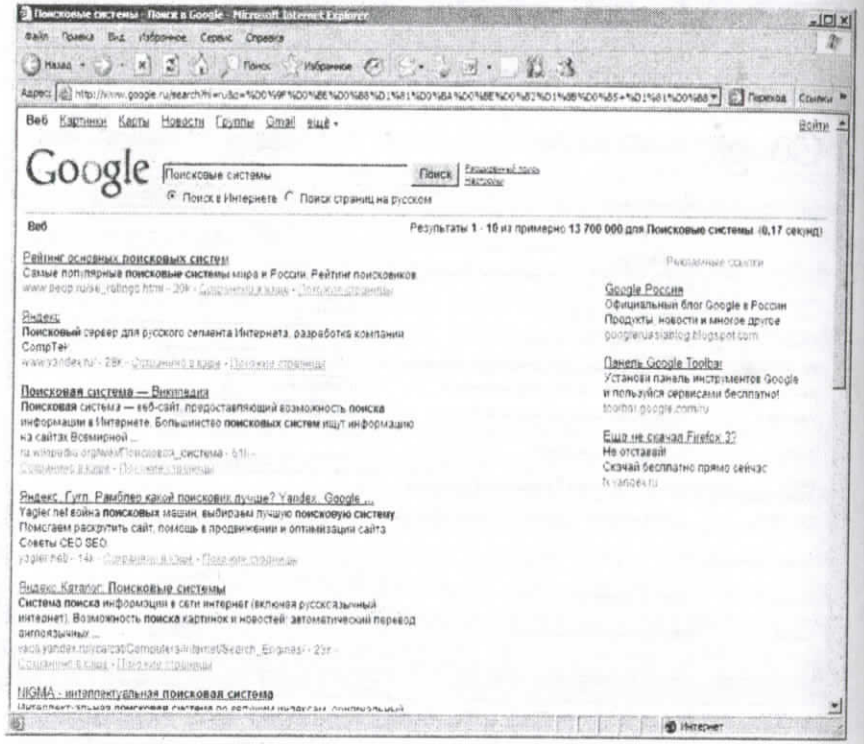



Рис.8.37. Результаты поиска системы Google

Google предоставляет пользователю разнообразные возможности по настройке интерфейса системы и непосредственно самих поисковых функций. На домашней странице имеется ссылка на страницу создания предустановок поиска: «Настройки» и «Языковые инструменты». Google поддерживает интерфейсы на 43 языках и позволяет открывать каждый найденный документ в новом окне браузера. Пользователь может задать поиск документов одновременно на нескольких языках, регулировать количество результатов поиска, выводимых на одну страницу, а также подключать фильтр для документов, содержащих ненормативную лексику. Созданные предустановки запоминаются браузером и действуют в каждой поисковой сессии, пока не будут изменены.



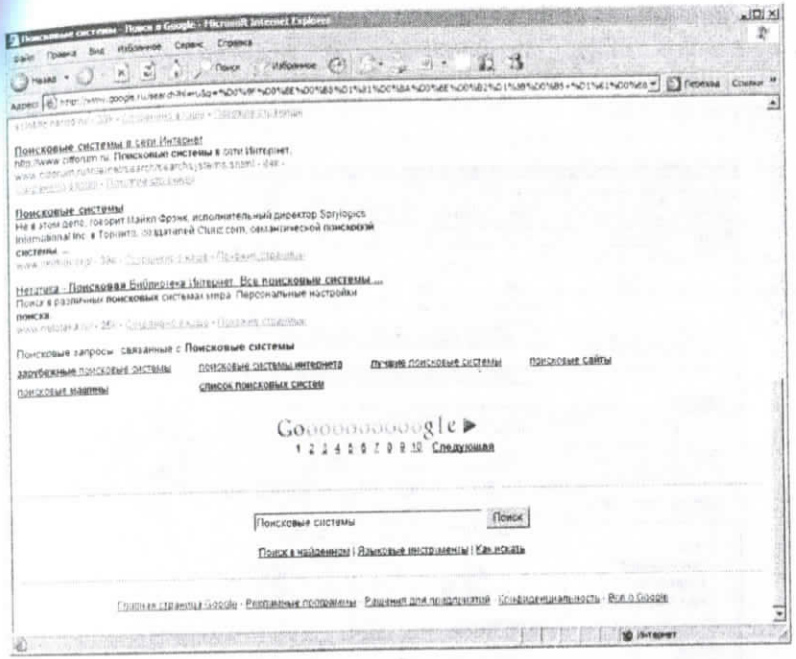



Рис.8.38. Формат выдачи результатов поиска системы Google

### 8.8.6. Поисковая система Rambler

Доступ к поисковой системе Rambler (http://www.rambler.ru) был открыт в 1996г. Это одна из первых российских поисковых систем, которая активно развивается. Система использует несколько одновременно работающих программ-роботов и обрабатывает около 5 пользовательских запросов в секунду.

Rambler представляет собой портал, объединивший поисковую систему, рейтинг-классификатор Rambler's Top100, а также ряд бесплатных сервисов и информационных проектов. Ресурсы портала регистрируют ежесуточно более 3,5млн. посещений. Наиболее интересными проектами являются «Rambler-Наука», «Интерактивные карты» и «Словари». Кроме того, пользователям предоставляется возможность проведения поиска информации на ftp-серверах (http://ftpsearch.rambler.ru:8101/).

Для поиска информации запрос из ключевых слов вводится в поисковое окно, расположенное в верхней части домашней страницы (рис.8.39). По умолчанию используется логический оператор «AND».

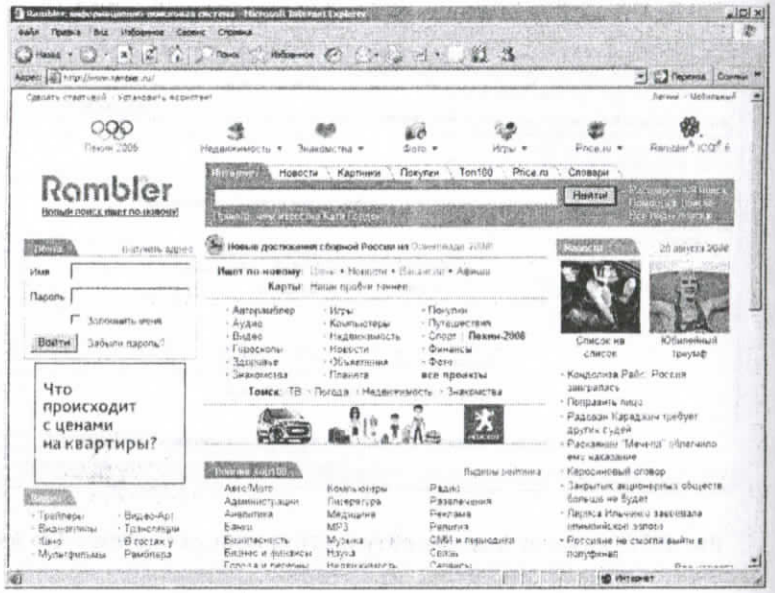



Рис.8.39. Домашняя страница поисковой системы Rambler

Система поддерживает составление запроса с использованием логических операторов «AND» («&») и «OR» («|»). Для составления сложного поискового выражения используются круглые скобки, задающие порядок действия операторов. Rambler поддерживает поиск по фразе. Фраза заключается в кавычки. Поиск морфологических форм задается оператором «#», а поиск однокоренных оператором «@». Поддерживается поисковая функция усечения справа и в середине слова. Символ «*» заменяет любое количество букв; символ «?» заменяет один неизвестный символ.

При составлении запроса можно использовать следующие специальные операторы:



**$All** – поиск во всех разделах html-документа;
**$URL** – поиск в URL-адресе html-документа;
**$Title** – поиск в заголовке html-документа;
**$Essence** – поиск в аннотации к html-документу.

Интерфейс страницы расширенного поиска содержит поле для ввода ключевых слов и шаблон, состоящий из нескольких фильтров для уточнения запроса (рис. 8.40).

Опция «Искать слова запроса:» содержит селекторные кнопки «все» и «хотя бы одно», заменяющие логические операторы «AND» и «OR». Чтобы исключить документы, содержащие те или иные слова, нужно заполнить поле «Исключить документы, содержащие хотя бы одно из следующих слов:».

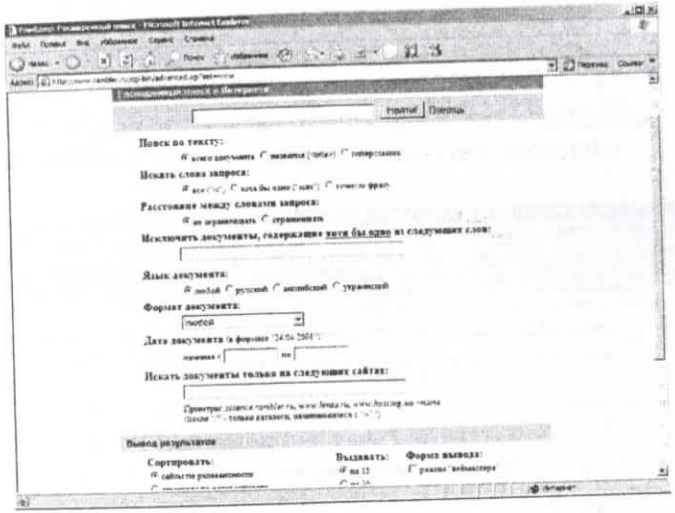


Рис.8.40. Интерфейс расширенного поиска системы Rambler

Система дает возможность о граничить поиск документами, созданными за определенный период времени. Ниже расположена область определения параметров сортировки и выдачи результатов поиска.

По умолчанию найденные документы сортируются по степени релевантности. Каждая страница может содержать от 15 до 50 ссылок на найденные документы (рис.8.41).

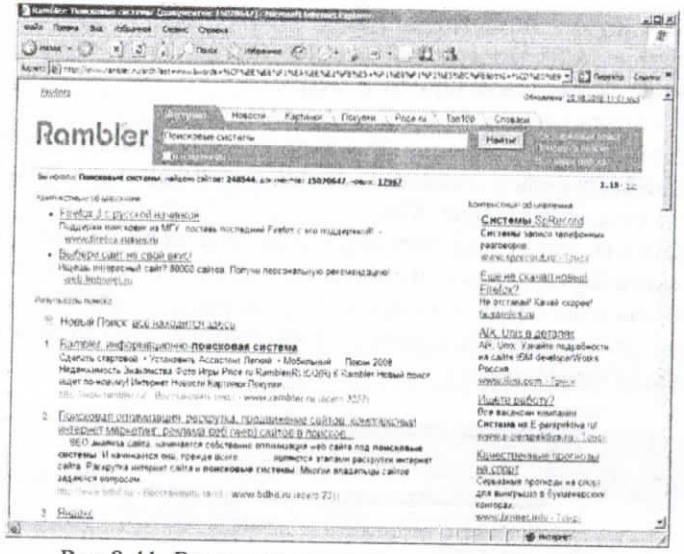



Рис.8.41. Результаты поиска системы Rambler

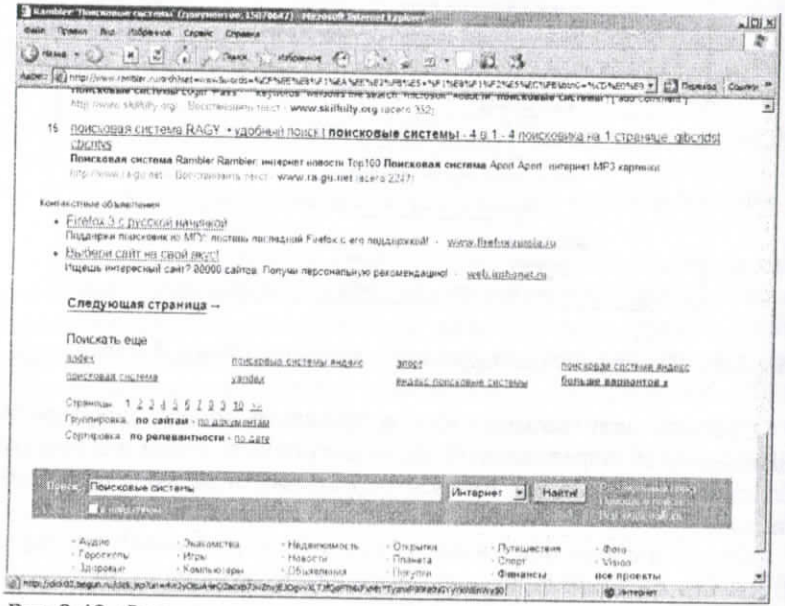


Рис.8.42. Формат выдачи результатов поиска системы Rambler



Полный формат выдачи результатов поиска состоит из следующих элементов: URL-адрес сайта, заголовок документа, выдержка из текста страницы с выделенными жирным шрифтом ключевыми словами, дата создания или последнего обновления документа, ссылки на другие поисковые системы (рис.8.42). Кроме того, указываются сведения о том, сколько всего найденных документов содержится на данном сайте.

## Контрольные вопросы

1. Каково назначение протоколов прикладного уровня?
2. Из каких компонентов состоит URL?
3. Как требования приложений к качеству передачи данных влияют на выбор протокола транспортного уровня?
4. В чём отличие принципа работы архитектуры «клиент-сервер» и архитектуры «точка-точка»?
5. Каково назначение сервиса E-mail?
6. Каково назначение Почтового сервера? Какие функции выполняют почтовые клиенты?
7. Из каких компонентов состоит структура почтового сообщения E-mail?
8. Что означает термин вложения (attachments) в сервисе E-mail?
9. Как осуществляется взаимосвязь протоколов Электронной почты с web-интерфейсом ?
10. Для чего предназначен сервис WWW?
11. Каково назначение HTTP?
12. Что обозначает термин «время оборота»?
13. Что такое объект web-страницы?
14. Каково назначение сервиса RTVC?
15. Что такое Видеоконференция?
16. Какие существуют типы видеоконференций в зависимости от уровня оборудования?
17. В чём отличие персональных, групповых и студийных видеоконференций?
18. Какие существуют типы видеоконференций по топологии?
19. Каково назначение протоколов семейства H.323?
20. Каково назначение сервиса SE?
21. Какие 3 самые популярные поисковые системы в зоне рунет?

22. Какие 3 основных международных поисковых системы?
23. Что обозначает термин «Релевантность документа»?
24. Что входит в состав Поисковой системы?
25. Что обозначает термин «Паук (spider)», «Путешествующий паук (crawler)», «оптимизатор» в Поисковой системе?
26. Каково назначение Поискового робота, Web-сервера, индексатора (indexer), базы данных (database) в Поисковой системе?
27. Каково назначение сервиса Usenet?
28. Что такое «Большая Восьмёрка» конференций Usenet?
29. Как выполняется загрузка и публикация файлов в Usenet?
30. Как долго хранится информация на серверах Usenet
31. Каково назначение сервиса IRC
32. Каково назначение каналов в IRC
33. Что такое IRC-боты, IRC-службы?
34. Кто такие операторы каналов в IRC? Кто становится Оператором канала?



## ГЛОССАРИЙ

| Термин на английском | Термин на русском | Определение на русском языке |
|---|---|---|
| Active document | Активный документ | в WWW - программа, выполняемая на стороне клиента. |
| Active open | Активное открытие | установление соединения между сервером и клиентом. |
| Address space | Адресное пространство | общее количество адресов, используемых в соответствии с протоколом, которое не связано непосредственно с применяемым программным обеспечением или размерами сети. |
| Alias | Групповое имя | в SMTP - имя, представляющее группу получателей. |
| Anycast address | Альтернативный адрес | адрес, который определяет группу компьютеров с адресами, имеющими один и тот же префикс. |
| Applet | Апплет | прикладная программа, запускаемая при каждом обращении к веб-странице, в исходный текст которой она встроена. |
| Application Layer | Прикладной уровень | самый верхний (седьмой) уровень эталонной модели ВОС (OSI), определяющий способы передачи информации между приложениями. На этом уровне обеспечивается взаимодействие с телекоммуникационными службами. |

| | | |
|---|---|---|
| ARP – Address Resolution Protocol | Протокол определения адресов | используется для динамического преобразования IP-адресов в физические (аппаратные) адреса устройств. |
| Authentication | Аутентификация | процедура установления прав и подтверждения полномочий вызывающего абонента, проводимая с целью определения принадлежности его к данной системе и проверки прав доступа к сетевым ресурсам. |
| Autonomous System - AS | Автономная система | группа сетей и маршрутизаторов, прикрепленная к одному-единственному администратору. |
| Autonomous system boundary router | Пограничный маршрутизатор автономных систем | отвечает за распространение информации об автономных системах в текущей системе. |
| Backbone Network | Магистральная сеть | совокупность сегментов сети, узлов и отдельных станций, которые подключаются к общей высокоскоростной линии связи через мосты, маршрутизаторы и концентраторы каналов. |
| Backbone router | Пограничный маршрутизатор зоны | машрутизаторы, устанав-ливаемые на границе зоны. |
| Banner | Баннер | рекламный фрагмент, обычно содержащий гиперссылку на другой сайт. |
| BGP – Border Gateway Protocol | Протокол пограничной маршрутизации | протокол маршрутизации между автономными системами, основанный на применении вектора пути. |



| | | |
|---|---|---|
| Binary notation | Двоичная система обозначений | метод представления информации, использующий только 0 и 1. |
| Block mode | Блочный режим | режим доставки данных от FTP к TCP в виде блоков. |
| Broadcast address | Широковещательный адрес | адрес для рассылки сообщений всем узлам сети. |
| Broadcasting | Широковещательная передача | метод передачи информации всем абонентам сети. |
| Browser | Браузер | программа поиска и чтения гипертекста. |
| Cache table | Кэш-таблица | таблица в протоколе ARP для временного хранения преобразованного номера. |
| Character mode | Символьный режим | режим работы TELNET, при котором каждый символ, напечатанный клиентом, посылается серверу. |
| Classfull addressing | Адресация по классам | адресация, применяемая в системе IPv4. При этом способе адресное пространство разделяется на 5 классов: A, B, C, D и E, каждый из которых занимает часть полногоадресного пространства (A - адреса, имеющие значение первого байтаот 0 до 127, B - от 128 до 191, C - от 192 до 223, D предназначен для мно-гоадресного использования и E зарезервирован для специальных целей). |

| | | |
|---|---|---|
| Classless InterDomain Routing, CIDR | Бесклассовая система междоменной маршрутизации | метод, применяемый для сокращения числа записей в маршрутизаторе, при котором маршрутизация осуществляется на основе префиксов. Префиксом обозначают общую часть старших разрядов адреса. |
| Client | Клиент | рабочая станция в сети, которая использует для своей работы ресурсы сетевого устройства (обычно сервера). |
| Client control process | Процесс управления клиентом | программа, выполняющая прикладную задачу на местной рабочей станции, которая запрашивает программу обслуживания удаленного компьютера. |
| Common Gateway interface - CGI | Общий шлюзовой интерфейс | интерфейс для поддержки однородного потока данных между сервером и клиентом, используемый при передаче информации веб-сервера к пользователю. |
| Compressed mode | Сжатый режим | режим доставки данных от FTP к TCP в сжатом виде. |
| Congestion | Перегрузка | состояние сети, при котором поступающая нагрузка превышает пропускную способность сети. |
| Connection | Соединение | в TCP/IP виртуальное соединение, устанавливаемое перед началом обмена сегментами между источником и пунктом назначения. Все сегменты, принадлежащие сообщению, затем посылаются этим виртуальным путем. |



| | | |
|---|---|---|
| Connectionless | Не ориентированный на соединение | способ организации связи, при котором предварительно не устанавливаются сквозные сетевые соединения и не гарантируется доставка информации. |
| Connection-oriented | Ориентированный на соединение | способ организации связи, при котором для начала передачи необходимо установить сквозное соединение между двумя станциями. |
| Control connection | Соединение для передачи сигналов управления | соединение FTP, которое используется для обмена управляющей информацией. |
| Convergence network | Конвергентная сеть | Конвергенция означает использование общей кабельной и коммутационной инфраструктуры для доступа к разрозненным серверам и сетям хранения информации |
| Cookies | | небольшой фрагмент данных, содержащих предысторию обращений данного пользователя к данному WWW-серверу; автоматически создается сервером на машине пользователя |
| Data compression | Сжатие данных | уменьшение объема данных за счет исключения избыточной информации или использования ее статистических особенностей. |

| | | |
|---|---|---|
| Datagram | Дейтаграмма | пакет данных, который пересылается по маршрутам сети независимо от остальной части информации, адресованной данному пользователю. |
| DDNS – Dynamic Domain Name System | Динамическая система доменных имен | метод изменения динамического (автоматического) мастер-файла DNS. |
| Defaul tmode | Режим, заданный по умолчанию | режим работы TELNET, который используется, когда с помощью опции переговоров не запрошены никакие другие режимы. |
| Direct delivery | Внутренняя маршрутизация | маршрутизация, при которой конечный пункт доставки пакета - хост, подключенный к той же самой физической сети, что и источник информации. |
| DNS – Domain Name System | Доменная система имен | Служба Интернет, осуществляющая присвоение уникальных имен всем узлам сети и позволяющая обрабатывать многочисленные запросы пользователей в реальном времени. |
| DNS-server | DNS-сервер | компьютер, который содержит информацию о пространстве имен. |
| Domain addresses | Символьные (доменные) адреса | адреса, которые предназначены для применения пользователями. Символьные адреса имеют сложную иерархическую структуру, содержащую имя |



| | | |
|---|---|---|
| | | пользователя, имя подсети (поддомена), символьное имя страны или организации (домена). |
| Domain Name Space | Пространство доменных имен | структура организации пространства имен, при которой имена определяются с помощью структуры инвертированного дерева с корнем и вершиной. |
| Dotted-decimal notation | Десятичная разделенная точками система обозначений | нотация, делающая IP-адрес более простым для чтения; каждый байт преобразуется в десятичный эквивалент и отделяется от соседней цифры. |
| Dynamic document | Динамический документ | документ, который создается веб-сервером всегда, когда браузер запрашивает документ. |
| Dynamic routing table | Динамическая таблица маршрутизации | таблица, используемая для маршрутизации, заполняемая автоматически в процессе устройствами маршрутизации. |
| Encryption | Шифрование | способ обработки данных, который обеспечивает охрану от неправомочного доступа (конфиденциальность), защиту от неправомочного изменения (целостность) и доступ только разрешенному объекту, когда это ему необходимо (готовность). |
| Error reporting | Отчет об ошибках | сообщение об ошибке, посылаемое источнику. |

| | | |
|---|---|---|
| ETSI | | Европейский Институт телекоммуникационных стандартов (ETSI) является независимой, неприбыльной организацией по стандартизации в телекоммуникационной отрасли (производители оборудования, операторы сетей) в Европе, со штаб-квартирой в София-Антиполис, Франция. |
| Four-way handshake | Метод взаимодействия в четыре шага | последовательность действий для установления и завершения соединения между клиентом и сервером за четыре шага. |
| FQDN – Fully Qualified Domain Name | Полностью определенное доменное имя | доменное имя, содержащее все метки, начиная от имени хоста и заканчивая меткой корневого узла. |
| Fragmentation | Фрагментация | разделение пакета на меньшие блоки для адаптации передачи к максимальному модулю передачи. |
| FTP – File Transfer Protocol | Протокол передачи файлов | протокол, который используется для передачи файлов от одного компьютера к другому. Обеспечивает просмотр каталогов удаленного компьютера, копирование, удаление и пересылку файлов. |



| | | |
|---|---|---|
| FTTx | | доведение оптического кабеля до квартиры жилого дома (The Apartment), здания (The Building), жилого дома (The Home), офиса (The Office) и т.д. |
| Generic domain | Родовой домен | поддомен в пространстве DNS-имен, который использует родовой суффикс. |
| Hello message | Сообщение "hello" | сообщение, которое используется в протоколе первоочередного открытия наикратчайших путей (OSPF)для создания отображения окружающей его сети и для проверки достижимости соседей. |
| Hierar chical name space | Иерархическое пространство имен | техника маршрутизации, при которой все пространство адресов разделено на уровни по определенным критериям. |
| HLEN – Header Length | Длина заголовка | поле IP-дейтаграммы на 4 бита, определяет полную длину дейтаграммного заголовка в 4-байтовыхсловах. |
| HTML – Hypertext Markup Language | Гипертекстовый язык | специальный язык для определения форматов текста, выбора расположения графических объектов, размера и цвета шрифта, включения видео и звука, запуска программ поиска документов и создания гиперссылок. |

| | | |
|---|---|---|
| HTTP – Hyper Text Transfer Protocol | Протокол передачи гипертекста | транспортный протокол, используемый в Интернете при обмене документами, которые представлены на языке описания гипертекстовых документов (HTML - HyperTextMarkupLanguage). Является одним из главных протоколов, используемых в сети WWW. |
| ICMP – Internet Control Message Protocol | Протокол управляющих сообщений Интернета - | протокол в стеке TCP/IP, отвечающий за организацию сеансов связи и восстановление межсетевых соединений после случайных сбоев. |
| IGMP | Протокол управления группами Интернета | протокол многоадресной рассылки в наборе протоколов TCP/IP, взаимодействует с протоколом IP. |
| IGMP – Internet Group Message Protocol | Межсетевой протокол управления группами | протокол в стеке TCP/IP для обработки групповых вызовов, обслуживает одновременную передачу сообщения к группе получателей. |
| Indirect delivery | Внешняя маршрутизация | маршрутизация, при которой пакет переходит от одного маршрутизатора к другому, пока не достигает физической сети, в которую включен конечный пункт. |
| Interface | Интерфейс | совокупность программных и аппаратных средств, а также правил, обеспечивающих их сопряжение на физическом и логическом уровне. |



| | | |
|---|---|---|
| Internet | Интернет | Всемирная сеть, объединяющая большое число трансконтинентальных национальных и локальных сетей с разной пропускной способностью и типами используемых каналов. |
| Internet Mail Access Protocol, Version 4 - IMAP4 | Протокол почтового доступа к сообщениям Интернета, версия 4 | протокол, обеспечивающий возможность интерактивного доступа к электронной почте. |
| IP – Internet Protocol | Протокол межсетевого взаимодействия | протокол сетевого уровня, входящий в стекTCP/IP, управляющий передачей и приемом на сетях с пакетной коммутацией без установления соединения. |
| IP-address | Интернет-адрес | адрес, который присваивается узлам сети, построенной на базе протоколов TCP/IP. |
| IP-notation | Система обозначений адреса IP | система обозначений, которая применяется, чтобы указать адресIP. Есть три общих системы обозначений: двоичная система, десятичная разделенная точками система обозначений и шестнадцатеричная система обозначений. |
| IPv6 | Интернет-протокол версии 6 | Интернет-протокол версии 6 (IPv6) - это самая последняя версия Интернет-протокола (IP) |
| Iterative resolution | Итерационное распознавание | Распознавание IP-адреса, при котором клиент посылает запрос к серверу, чтобы получить вответадрес. |

| | | |
|---|---|---|
| Jitter | Джиттер | при передаче нагрузки в реальном масштабе времени случайное изменение времени следования последовательных пакетов по сравнению с исходным временем посылки их передатчиком. |
| Keepalive message | Дежурное сообщение | сообщение, которое подтверждает наличие соединения между двумя маршрутизаторами. |
| Link Layer | Канальный уровень | второй уровень эталонной модели взаимодействия открытых систем, который является передаточной средой между сетевым и физическим уровнем. |
| Link State Database | База данных состояния связи | таблица, представляющая топологию Интернета внутри зоны. Она показывает связь между каждым маршрутизатором и соседним к нему, включая метрику. |
| Link State Packet | Пакет запроса состояния линейки | пакет, который посылается маршрутизатором, нуждающимся в информации о маршрутах. Другие маршрутизаторы на него отвечают пакетом с обновлением состояний линий. |
| Linkstate packet | Пакет подтверждения состояния связи | пакет подтверждения пакета обновления состояния линии. Применяется каждым маршрутизатором для подтверждения каждого пакета обновления. |



| | | |
|---|---|---|
| Local Network | Локальная сеть | небольшая группа узлов, связанная единым адресным пространством. Примеры локальных сетей: Ethernet, TokenRing. |
| Login | Логин | автоматическая проверка введенного пользователем пароля и прав доступа к запрашиваемым ресурсам системы |
| Loopback | Адрес шлейфа | адрес для проверки программного обеспечения компьютера. Когда этот адрес используется, пакет никогда не покидает хост; он просто возвращается к нему и обрабатывается согласно протоколу и установленному на управляющем компьютере программному обеспечению. |
| Loopback address | Адрес кольцевой проверки | адрес, используемый хостом для проверки собственного программного обеспечения. |
| Mail Transfer Agent | Агент почтовой передачи | программа электронной почты (компонент SMTP), действующая от имени сервера и обеспечивающая цикл операций, которые связаны с передачей, обработкой и доставкой сообщений. |
| Manager | Менеджер | программа, управляющая процессом выполнения других программ. В SNMP она размещается в хосте и выполняет функции программы SNMP-клиента. |

| | | |
|---|---|---|
| Mask | Маска | кодовая комбинация (шаблон), используемая для изменения данных (адреса) путем поэлементного логического умножения ее элементов с изменяемой информацией (адресом). |
| Mask request and replay | Запрос маски адреса и ответ | ICMP-запрос, который посылается хостом. Чтобы получить свою маску, хост посылает сообщение запроса маски-адреса маршрутизатору местной сети. |
| Metric | Метрика | условная стоимость передачи по сети. |
| MIB – Management Information Base | База управляющей информации | информационная база данных, которая содержит текущую, разбитую на категории информацию обо всех контролируемых и управляемых устройствах, подключенных к сети. Применяется как компонент протокола SNMP. |
| Mixing | Смешивание | в системах реального времени математическое сложение сигналов, поступающих от различных источников, для того чтобы создать единственный сигнал. |
| Module | Модуль | программно-аппаратное унифицированное средство, входящее в состав узла, имеющее средства сопряжения с другими модулями и реализующее |



| | | |
|---|---|---|
| | | определенную функцию (протокол). Может одновременно входить в состав другого модуля. Примеры модуля: модульIP, модульICMP. |
| MSS – Maximum segment size | Максимальный размер сегмента | опция, определяющая размер наибольшего кванта данных, который может быть получен пунктом назначения сегмента TCP. |
| MTU | Максимальный модуль передачи | наибольший размер блока данных, заданный для сети, который может быть обработан. |
| Multicasting | Многоадресная передача | передача информации в несколько пунктов или по нескольким адресам (см. Широковещательная передача). |
| Multicasting | Циркулярное сообщение | передача информации в несколько пунктов или адресов, обычно объединенных в адресные группы. |
| Multipurpose Internet Mail Extensions - MIME | Многоцелевое расширение интернет-почты | протокол, позволяющий передавать мультимедийные, графические сообщения и другие нетекстовые данные, используя SMTP-данные, которые не имеют вид ASCII. |
| Network Layer | Сетевой уровень | третий уровень эталонной модели взаимодействия открытых систем, который обеспечивает адресацию и маршрутизацию информационных потоков. |

| | | |
|---|---|---|
| Network Virtual Terminal | Виртуальный сетевой терминал | протокол набора TCP/IP, позволяющий проводить удаленный логин, который осуществляет преобразование символов TELNET-клиента к универсальному набору и доставляет их протоколам TCP/IP. |
| NFS – Network File System | Сетевая файловая система | система, которая позволяет использовать файлы, расположенные на другом компьютере, так же как собственные файлы. |
| Node | Узел | любой сетевой элемент, имеющий хотя бы один сетевой адрес (IP-адрес). Примеры узла: оконечное устройство (хост), маршрутизатор, шлюз. |
| Notification message | Сообщение уведомления | сообщение, которое посылается маршрутизатором, выполняющим протокол BGP, когда обнаружены признаки ошибки или маршрутизатор завершает соединение. |
| Open System | Открытая система | стандартизированный набор протоколов и интерфейсов, который гарантирует возможность взаимодействия оборудования различных производителей. |
| OSI – Open System Interconnection | Взаимодействие открытых систем - ВОС | концептуальная основа, которая определяет характеристики и свойства семейства стандартов, разработанных ISO на базе семиуровневой модели протоколов. |



| | | |
|---|---|---|
| OSPF – Open Shortest Path First | "Открыть кратчайший путь первым" | внутрисетевой протокол маршрутизации, основанный на анализе состояния линий связи. |
| Out-of-band signaling | Передача сигналов вне полосы | метод, при котором управляющие сигналы и данные проходят по разным каналам. |
| Packet | Пакет | структурированная информация, передаваемая и обрабатываемая как единое целое, имеющая IP-адрес и полезную нагрузку. |
| Passive open | Пассивное открытие | состояние сервера, когда он ждет входящего запроса от клиента. |
| Path vector routing | Маршрутизация с использованием вектора путей | метод маршрутизации, применяемый в протоколе пограничной маршрутизации (BGP); основан на подробном описании с помощью вектора путей автономных систем, через которые должен пройти пакет. |
| Physical address | Физический адрес | адрес устройства, используемый для маршрутизации (MAC-адрес). |
| Physical Layer | Физический уровень | самый нижний уровень (первый уровень) эталонной модели ВОС (OSI), который обеспечивает физическую и электрическую связь между абонентским и оконечным сетевым оборудованием. |
| Playback buffer | Буфер воспроизведения | буфер, который сохраняет информацию до тех пор, пока она не будет готова к воспроизведению. |

| | | |
|---|---|---|
| Point-to-Point | Связь "точка-точка" | соединяет два маршрутизатора без участия любого другого хоста или маршрутизатора между ними. |
| Policy routing | Политика маршрутизации | набор правил, назначаемых администратором, который управляет в протоколе пограничной маршрутизации (BGP) формированием таблиц маршрутизатора. |
| Port | Порт | Многоразрядный вход/выход, служащий для подключения внешнего оборудования, или интерфейс взаимодействия между двумя устройствами на физическом уровне. Может иметь закрепленный за ним сетевой адрес. Примеры портов: E1, T1, E3, T3). Интерфейс, с помощью которого два устройства могут связать друг с другом и обмениваться данными |
| Port Address | Адрес порта | в архитектуре TCP/IP метка, назначаемая процессу; используется для коммутации процесса, работающего с другим процессом. |
| Post Office Protocol Version 3 - POP3 | Почтовый протокол версии 3 | почтовый протокол, регламентирующий процедуру пересылки почтовой корреспонденции только от сервера к клиенту. |
| Precedence | Биты категории срочности | подполе заголовка IP-дейтаграммы на 3 бита, определяющее приоритет дейтаграммы в случае перегрузки. |



| | | |
|---|---|---|
| Presentation Layer | Представительный уровень | шестой уровень эталонной модели взаимодействия открытых систем, который определяет способ представления (синтаксическую структуру) данных в процессе обмена между двумя прикладными процессами или конечными пользователями. |
| Process | Процесс | работающая прикладная программа, т. е. последовательность смены состояний объекта при поступлении внешних входных сигналов и заданного алгоритма их обработки. |
| Protocol | Протокол | набор формализованных правил, процедур и спецификаций, определяющих формат и способ передачи данных. |
| Proxy server | Сервер-посредник | компьютер, который содержит программные средства, предназначенные для защиты локальной и корпоративной сети от несанкционированного доступа или опасных приложений. |
| Pseudo header | Псевдозаголовок | заголовок пакета, к которому добавлены вспомогательные данные (например, контрольная сумма). |
| Pushing data | Проталкивание данных | метод, при котором данные, требующие минимальной задержки, маркируются ответом в специальном бите заголовка TCP/IP. |

| | | |
|---|---|---|
| Queue | Очередь | последовательный список элементов, организуемый для выполнения определенного алгоритма их обработки. |
| RARP - Reserve Address Resolution Protocol | Протокол определения сетевого адреса по местоположению | протокол обратного преобразования, используемый для динамического преобразования физических адресов устройств в IP-адреса. |
| Real-time traffic | Нагрузка (трафик) в реальном масштабе времени | одна из форм нагрузки, при которой данные одновременно производятся на передаче и используются на приеме (пренебрегая временем прохождения по каналам связи). |
| Real-time Transport Protocol - RTP | Транспортный протокол реального масштаба времени | протокол передачи потоковой мультимедийной информации, использующий UDP реального масштаба по IP-сетям. |
| Real-timeTransport Control Protocol - RTCP | Транспортный протокол управления реального масштаба времени | протокол, управляющий потоком и качеством передачи данных, который позволяет иметь обратную связь при передаче сообщений от источника к источнику. Работает совместно с RTP. |
| Record Route | Опция записи полного маршрута | опция, используемая для записи маршрутов, которые обрабатывают дейтаграмму. |
| Redirection | Переадресация | перенаправление вызова или документа по другому адресу. |



| | | |
|---|---|---|
| Resolver | Распознаватель | сервер клиент DNS, который используется хостом, когда необходимо отобразить IP-адрес в имя или имя в адресIP. |
| RIP – Routing Information Protocol | Протокол обмена маршрутной информацией | протокол маршрутизации, основанный на использовании алгоритма вектора расстояний. |
| RIP – Routing Information Protocol | Протокол обмена маршрутной информацией | протокол маршрутизации, основанный на использовании алгоритма вектора расстояний. |
| Router | Маршрутизатор | узел, который осуществляет выбор маршрута и ретранслирует пакеты между интерфейсами в соответствии с сетевым адресом. Имеет не менее двух физических интерфейсов. Иногда маршрутизатор называют шлюзом. |
| Routing | Маршрутизация | процедура выбора пути транспортировки информации от отправителя к получателю с заданным качеством и минимальными задержками; также процесс доставки по этому пути. |
| Routing table | Таблица маршрутизации | таблица, которая показывает стоимость достижения каждого узла в зоне. Она может содержать: сетевой адрес, стоимость достижения, адрес следующего участка и другую информацию. |
| Segment TCP/IP | Сегмент в TCP/IP | часть потока данных, вырезаемая из входного буфера. |

| | | |
|---|---|---|
| Segmentation | Сегментация | разбиение массива данных на фрагменты, которые можно обрабатывать отдельно друг от друга. |
| Server | Сервер | узел сети, специализированная станция или процессор, с помощью которых обеспечивается обслуживание рабочих станций, терминалов и других устройств, а также предоставление им коллективно используемых ресурсов. |
| Session Layer | Сеансовый уровень сеанса | пятый уровень эталонной модели взаимодействия открытых систем, который определяет способы установки, поддержания и разрыва соединения. |
| Silly window syndrom | Синдром "глупого окна" | ситуация, при которой передающая прикладная программа медленно создает данные, либо приемная прикладная программа медленно принимает данные, либо имеют места оба случая. |
| Simple data type | Простой тип данных | тип данных в SMI, который состоит из частей других типов данных. |
| Simple Mail Protocol | Простой почтовый протокол SMTP | протокол передачи сообщений, применяемый в сетях на базе стека протоколов TCP/IP. Поддерживает режим передачи 7-битовых слов только в каналах с немедленной отправкой сообщений, в которых получатель постоянно готов к получению почты. |



| | | |
|---|---|---|
| SIP – Session Initializing Protocol | Протокол инициализации сеанса связи | протокол сигнализации, используемый в системах компьютерной телефонии, мобильных сетях и многосторонней конференц-связи. Предназначен для вызовов с автоматическим определением местоположения вызываемой стороны. |
| Slow start | Медленный старт | метод управления перегрузкой, при котором размер окна перегрузки сначала увеличивается экспоненциально. |
| SMI – Structure of Management Information | Структура управляющей информации | набор правил для описания в терминах ASN.1 и идентификации переменных. |
| SMTP – Simple Mail Protocol | Простой почтовый протокол | поддерживает передачу почтовых электронных сообщений по сети Интернет. Протокол называется простым, потому что обеспечивает передачу информации пользователям, готовым к немедленной доставке. Передача осуществляется в режиме 7-битовых слов. |
| SNMP – Simple Network Management Protocol | Простой протокол управления сетью | обеспечивает набор фундаментальных действий по наблюдению и обслуживанию Интернета. Протокол разработан так, чтобы он мог контролировать устройства, сделанные различными изготовителями и установленные на различных физических сетях. |

| | | |
|---|---|---|
| SNMP – Simple Network Management Protocol | Простой протокол управления сетью | протокол семейства TCP/IP, использующий информационную базу о сетевых объектах для запоминания их состояний и отслеживания состояния сетевого трафика. |
| Spooling | Буферизация | процесс ввода-вывода с использованием буферной памяти, осуществляемый параллельно с исполнением текущей задачи. |
| Static document | Статический документ | в WorldWideWeb - документ с фиксированным содержанием, который создан и сохраняется всервере. |
| Static Routing Table | Статическая таблица маршрутизации | таблица, используемая для маршрутизации и заполняемая обслуживающим персоналом. |
| Stream Control Transmission Protocol - SCTP | Транспортный протокол управления потоком данных | транспортный протокол, разработанный для IP-телефонии и соответствующих приложений. |
| Stream mode | Поточный режим | режим передачи FTP, при котором данные доставляются от FTP к TCP как непрерывный поток байтов. |
| Stream, flow | Поток | непрерывная последовательность данных, передаваемых по каналу или линии связи. |
| TCP | Протокол управления передачей | достоверный транспортный протокол потока в стеке протоколов TCP/IP, |



| | | |
|---|---|---|
| | | ориентированный на дуплексный режим связи с установлением логического соединения. Передача осуществляется путем разбиения потока на части (сегменты). |
| TCP/IP stack | Стек протоколов сети Интернет | протоколы управления сетями Интернет, которые включают в себя протоколы сетевого уровня (IP), транспортного уровня (TCP и UDP), прикладного уровня. |
| TERminal NETwork | TELNET | стандартный протокол TCP/IP для услуг виртуального терминала, имитации работы местного терминала на удаленном компьютере. |
| TFTP - TrivialFileTransferProtocol | Тривиальный (простейший) протокол передачи файлов | протокол, который используется для начальной загрузки рабочих станций и поддерживает обмен данными без аутентификации пользователя. |
| Three-way handshake | Метод взаимодействия в три шага | последовательность действий для установления или завершения соединения, которая состоит из запроса, подтверждениязапроса, подтверждения завершения. |
| Time stamp | Метка времени | данные, вставляемые в структуру сообщения при передаче нагрузки в реальном масштабе времени, которые указывают время создания относительно первого (или предыдущего) пакета. |

| | | |
|---|---|---|
| timeexceededmessage | Сообщение "время истекло" | ICMP-сообщение об ошибке, которое посылается к источнику, когда значениеполя"время жизни" равно нулю или фрагмент сообщения не был получен в течение заданного времени. Это сообщение отправляется хосту или маршрутизатору, участвующему в объединении определенной группы. |
| Translation | Трансляция в системах реального времени | процесс изменения кода или протокола на другой. |
| Transport Layer | Транспортный уровень | четвертый уровень эталонной модели взаимодействия открытых систем, который определяет способы транспортировки информации между конечными пунктами сети. |
| Trigger edupdate process | Запускаемое обновление | обновление в протоколе обмена маршрутной информацией (RIP), которое запускается через заданные интервалы времени. |
| Trivial File Transfer Protocol - TFTP | Простейший протокол передачи файлов | упрощенная версия протокола FTP, которая обычно применяется для начальной загрузки рабочих станций (клиентов). |
| TTL – time-to-live | Время жизни | параметр, определяющий время, при котором накопленная или передаваемая информация действительна. |



| | | |
|---|---|---|
| Type-of-Service - TOS | Тип сервиса | полеIP-дейтаграммы, определяющее ее обработку. |
| UDP – User Datagram Protocol | Протокол пользовательских дейтаграмм | протокол транспортного уровня в стеке протоколов TCP/IP. Он выполняет функции передачи между прикладными уровнями разных рабочих станций без установления соединения, по адресу порта, контролирует ошибки по контрольной сумме и передает информацию верхним уровням. |
| UE | | Пользовательское оборудование - это любое устройство, используемое непосредственно для конечных пользователей для общения. Это может быть ручное телефон, портативный компьютер оснащен мобильный широкополосный адаптер, или любого другого устройства. |
| Unicast address | Индивидуальный адрес | адрес, принадлежащий одному пункту назначения. |
| Urgent data | Срочные данные | в TCP/IP - данные, которые должны быть доставлены прикладной программе как можно скорее. |
| URL – Uniform Resource Locator | Универсальный идентификатор ресурса | стандартный формат представления логического адреса информационных ресурсов в сети Интернет. |
| User Datagram | Пользовательские дейтаграммы | пакеты UDP, которые пересылаются по сети независимо от другой информации, посылаемой тому же пользователю. |

| | | |
|---|---|---|
| User interface | Пользовательский интерфейс | интерфейс между пользователем и приложением. |
| UserAgent - UA | Агент пользователя | программа электронной почты (компонент SMTP), действующая от имени пользователя и обеспечивающая цикл операций, которые связаны с передачей, обработкой и доставкой сообщений (подготовка сообщения, оформление адресов и размещение текста). |
| Utility program | Утилита | сервисная программа, обеспечивающая выполнение некоторых служебных функций. |
| Vector routing | Вектор пути | вектор, определяющий маршрут доставки дейтаграмм, включает в себя указатели на все узлы, расположенные на пути следования. В литературе встречается название "вектор рас-стояний" (distancevector). |
| Virtual link | Виртуальная линия | соединение, которое создает администратор, когда выходит из строя физическая линия между двумя маршрутизаторами; при этом оно может использовать более длинный путь, который вероятнее всего пройдет через несколько маршрутизаторов. |
| Web-page | Веб-страница | документ, составленный на языке HTML и являющийся основой информационного обмена в сети Интернет. |



| | | |
|---|---|---|
| Web-server | Веб-сервер | узел в сети Интернет, предназначенный для обработки запросов пользователей и предоставления запрашиваемых HTML-документов. |
| WorldWideWeb - WWW | Всемирная паутина | глобальная гипертекстовая информационная система, объединяющая огромное количество гипертекстовых и иных документов, которые хранятся во многих странах мира и доступны через веб-узлы по каналам связи. |
| Agent | Агент | любое устройство или программа, которые действуют от имени и под управлением другой программы или устройства. В SNMP -программа маршрутизатора или хоста, выполняющая функции SNMP-сервера. |
| MAC – Media Access Control Adress | Адрес доступа | физический(аппаратурный) адрес, используемый для маршрутизации и обеспечивающий доступ к заданному устройству или группе устройств. |

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ


1. Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. 2017.
2. Мирзиёев Ш.М. Қонун устуворлиги ва инсон манфаатларини таъминлаш - юрт тараққиёти ва халқ фаровонлигининг гарови. 2017.
3. Мирзиёев Ш.М. Танқидий таҳлил, қатъий тартиб-интизом ва шахсий жавобгарлик – ҳар бир раҳбар фаолиятининг кундалик қоидаси бўлиши керак. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2016 йил якунлари ва 2017 йил истиқболларига бағишланган мажлисидаги Ўзбекистон Республикаси Президентининг нутқи. // Халқ сўзи газетаси. 2017 йил 16 январь, №11.
4. Мирзиёев Ш.М. "Тошкент ахборот технологиялари университетининг фаолиятини янада такомиллаштириш чора-тадбирлари тўғрисида" га қарори. ПҚ-2834, 15.03.2017.
5. Ўзбекистон Республикасини янада ривожлантириш бўйича харакатлар стратегияси тўғрисида. Ўзбекистон Республикаси Президентининг ПФ-4749-сон фармони. Тошкент, 2017 йил 7 феврал.
6. J.Kurose, K.Ross. Computer networking. Sixth edition. Pearson Education, 2013.
7. M.Naugle. Illustrated TCP/IP. A graphic guide to the protocol suite. John Wiley & Sons, Inc. – 480.
8. В.Олифер, Н.Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010.
9. В.П. Комагоров. Технологии сети Интернет: протоколы и сервисы. – Томск: Томский политехнический университет, 2009. – 107с.
10. В.П. Комагоров. Архитектура сетей и систем телекоммуникаций. Учебное пособие. – Томск: Томский политехнический университет, 2008. – 147с.
11. Таненбаум Э. Компьютерные сети. Изд.4. /Изд. Питер, 2003
12. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. Ташкент. ТУИТ.2008
13. Садчикова С.А., Абдужаппарова М.Б. Интернет сети и услуги. Методическое пособие для практических занятий /ТУИТ. 210 с. Ташкент, 2017
14. Хомоненко А.Д. Основы современных компьютерных технологий: Учебник для ВУЗ. – С-Пб.: Корона-принт, 2006 г.
15. Алимова Г.Б. История развития Интернета в Узбекистане: детали, прогнозы // Проблемы филологии, культурологии и искусствоведения в свете современных исследований: сборник материалов 18 международ. науч.-практ. конф. – Махачкала: Издательство «Апробация», 2016. – с.42-44.
16. Н.В. Кандаурова, С.В. Яковлев, В.П. Яковлев, В.С. Чеканов. Вычислительные системы, сети и телекоммуникации. Курс лекций и лабораторный практикум) : учебное пособие. – М. : Флинта, 2013. – 344 с.
17. С.Шатт. Мир компьютерных сетей, пер. с англ. - К.: BHV, 2004 г.
18. Галкин В.А., Ю.А. Григорьев. Телекоммуникации и сети. Учебник для бакалавров направлений «Информационные технологии». Москва, МГТУ им. Н.Э.Баумана, 2003
19. Еркинбаева Л.Т., Садчикова С.А., Каюмова Г.А. Телекоммуникационные системы и сети. Методическое пособие для проведения практических занятий. ТУИТ. Ташкент 2012.
20. Эшмурадов А.М., Садчикова С.А., Зайнутдинова Н.А Системы коммутации. Учебное пособие. Ташкент, 2011.
21. Садчикова С.А. Еркинбаева Л.Т. Сон В.М. Сети связи следующего поколения NGN. Часть 1. Протоколы сети NGN. Методическое пособие для практических занятий/ ТУИТ. Ташкент 2009.

Интернет сайты

22. Материалы курса «Основные протоколы интернет» сайта Интернет-Университета Информационных Технологий http://www.intuit.ru/studies/courses/2/2/info
23. Материалы курса «Локальные сети и интернет» сайта Интернет-Университета Информационных Технологий http://www.intuit.ru/studies/courses/509/365/info
24. Материалы курса «IP-телефония в компьютерных сетях» сайта Интернет-Университета Информационных Технологий http://www.intuit.ru/studies/courses/8/8/info
25. Шарифов Р.А. Садчикова С.А. Тилляев С.Д. IP-телефония. Методическое пособие лабораторных работ по дисциплине «IP-телефония» для магистрантов специальностей 5А522202,

5A522203, 5A522205, 5A522216. Ташкент, ТУИТ. 2008. http://www.teic.uz/lib
26. Шарифов Р.А., Садчикова С.А. Методическое пособие для практических занятий по предмету «IP-телефония». Ташкент, ТУИТ, 2008
27. Садчикова С.А. Сети связи следующего поколения NGN. Конспект лекций. Ташкент, ТУИТ. 2011. 275с. http: // www. teic.uz/ lib
28. Эшмурадов А.М., Садчикова С.А. Норматова Д.Т. Технологии сетей связи следующего поколения. Методическое пособие по дисциплине ЦСК-2. Ташкент,/ТУИТ. 2011. 275с. http: // www. teic.uz/ lib
29. http://lex.uz/pages/GetAct.aspx?lact_id=314306
30. http://www.medialawca.org/document/-1791



## ОГЛАВЛЕНИЕ

**ПРЕДИСЛОВИЕ** ..... 7
**ВВЕДЕНИЕ** ..... 9
**1. КОМПЬЮТЕРНЫЕ СЕТИ И ИНТЕРНЕТ** ..... 11
1.1. Введение – что такое Интернет? ..... 11
1.2. История возникновения сети Интернет ..... 14
1.2.1. Появление Интернет в Узбекистане ..... 18
1.3. Принципы построения сети Интернет ..... 20
1.4. Основные понятия и определения, используемые при работе в Интернет ..... 26
1.5. Стандарты в сфере Интернет ..... 31
1.6. Обобщённая структура телекоммуникационной сети с точки зрения сети Интернет ..... 33
1.6.1. Понятие о системах электросвязи ..... 33
1.6.2. Обобщённая структура телекоммуникационной сети ..... 34
1.6.3. Методы классификации компьютерных сетей .. 37
1.6.4. Сети операторов связи и корпоративные сети .. 42
**Контрольные вопросы** ..... 45
**2. СПОСОБЫ ПОДКЛЮЧЕНИЯ К ИНТЕРНЕТ** ..... 46
2.1. Виды сетей доступа ..... 46
2.2. Dial-up доступ ..... 48
2.3. Доступ xDSL ..... 49
2.4. Кабельный доступ HFC ..... 52
2.5. Доступ FTTx ..... 52
2.6. Корпоративный доступ ..... 60
2.7. Мобильный доступ ..... 60
2.8. Доступ в Интернет через спутниковые каналы ..... 67
2.9. Телекоммуникационные линии связи ..... 68
2.9.1. Кабельные линии ..... 69
2.9.2. Волоконно-оптический кабель ВОЛС ..... 72
2.9.3. Радиоканалы ..... 74
**Контрольные вопросы** ..... 79
**3. ЛОКАЛЬНЫЕ СЕТИ И ИХ КОМПОНЕНТЫ** ..... 80
3.1. Локальные сети – общие понятия ..... 80
3.2. Сетевое программное обеспечение ..... 82
3.3. Сетевая операционная система ..... 84
3.4. Типовой состав оборудования локальной сети 85

3.5. Уровневая модель локальной сети 87
3.5.1. IEEE 802.3 – LAN Ethernet 92
3.5.2. IEEE 802.4 – LAN ARCnet 94
3.5.3. IEEE 802.5 – LAN Token Ring 95
3.6. FDDI – технология глобальной сети WAN 97
3.7. Беспроводные WLAN стандарта 802.11 ..... 99
**Контрольные вопросы** ..... 104
**4. КОММУТАЦИЯ И МАРШРУТИЗАЦИЯ В ИНТЕРНЕТ СЕТЯХ** ..... 105
4.1. Коммутация определение ..... 105
4.2. Информационный поток – определение ..... 107
4.3. Коммутация пакетов ..... 107
4.4. Обработка пакета в маршрутизаторе ..... 109
4.4.1. Дейтаграммная передача ..... 111
4.4.2. Передача с установлением логического соединения ..... 112
4.4.3. Передача с установлением виртуального канала ..... 113
4.5. Коммутация каналов ..... 114
4.5.1. Пример мультиплексирования – структура первичного цифрового потока E1 ..... 118
4.6. Маршрутизация в интернет сетях ..... 121
**Контрольные вопросы** ..... 123
**5. СТЕК ПРОТОКОЛОВ TCP/IP И МОДЕЛЬ OSI** ..... 125
5.1. Многоуровневая модель обслуживания протоколов ... 125
5.2. Стек протоколов Интернета ..... 127
5.2.1. Прикладной уровень ..... 128
5.2.2. Транспортный уровень ..... 128
5.2.3. Сетевой уровень ..... 130
5.2.4. Канальный уровень ..... 130
5.2.5. Физический уровень ..... 131
5.3. Эталонная модель взаимодействия открытых систем ВОС (OSI) ..... 131
5.4. Инкапсуляция данных ..... 133
5.5. Адресация TCP/IP. Типы адресов в IP-сетях ..... 135
5.5.1. Адресация в IPv6 ..... 141
5.6. DNS – система доменных имен, принципы их распределения и распознавания ..... 143
5.6.1. Служба трансляции имен Интернета – функции DNS ..... 143
5.6.2. Общие принципы функционирования DNS ..... 145
5.6.3. DNS-записи и DNS-сообщения ..... 149
**Контрольные вопросы** ..... 150
**6. ПРОТОКОЛЫ СЕТЕВОГО УРОВНЯ TCP/IP** ..... 152
6.1. Функции сетевого уровня ..... 152
6.2. Интернет-протокол IP – основной протокол сетевого уровня ..... 154
6.2.1. Фрагментация IP-дейтаграмм ..... 158
6.3. Протокол определения адресов (ARP) и протокол определения сетевого адреса по местоположению (RARP) ..... 162
6.3.1. Передача дейтаграммы узлу в пределах локальной сети ..... 165
6.3.2. Передача дейтаграммы узлу за пределы локальной сети ..... 168
6.4. Протокол управления сообщениями Интернета (ICMP) ..... 170
**Контрольные вопросы** ..... 174
**7. ПРОТОКОЛЫ ТРАНСПОРТНОГО УРОВНЯ TCP/IP** ... 175
7.1. Функции транспортного уровня ..... 175
7.2. Пользовательский протокол дейтаграмм UDP ..... 177
7.2.1. Контрольная сумма UDP сегмента ..... 180
7.3. Протокол управления передачей TCP ..... 182
7.3.1. Принципы надежной передачи данных и TCP-соединение ..... 182
7.3.2. Структура TCP-сегмента ..... 185
7.3.3. Сценарии работы TCP протокола ..... 189
7.4. Управление TCP-соединением ..... 192
**Контрольные вопросы** ..... 196
**8. ПРОТОКОЛЫ ПРИКЛАДНОГО УРОВНЯ TCP/IP** ..... 197
8.1. Функции прикладного уровня и принципы работы протоколов ..... 197
8.2. Взаимодействие процессов через сеть ..... 202
8.3. Службы, необходимые приложению ..... 204
8.4. Сервис Telnet – стандартный протокол для услуг виртуального терминала ..... 207
8.4.1. Пример выполнения лабораторной работы «Добавление ADSL профилей абонентов на

порту DSLAM с использованием протокола Telnet» ..... 209
8.5. Сервис FTP – система файловых архивов ..... 215
8.6. Сервис электронная почта (e-mail) ..... 217
8.6.1. Сравнение SMTP и HTTP ..... 220
8.6.2. Форматы сообщений электронной почты и MIME ..... 221
8.6.3. Протоколы доступа к электронной почте ..... 223
8.6.4. Электронная почта с web-интерфейсом ..... 227
8.7. Сервис World Wide Web – гипертекстовая система интеграции сетевых ресурсов в единое информационное пространство ..... 229
8.7.1. Web и HTTP ..... 229
8.7.2. Обзор HTTP ..... 230
8.7.3. Постоянные и непостоянные соединения ..... 232
8.7.4. Формат HTTP-сообщений ..... 234
8.7.5. Взаимодействие пользователя с сервером – Cookie ..... 239
8.8. Сервис SE – поисковые системы ..... 242
8.8.1. Назначение сервиса SE ..... 242
8.8.2. Критерии ранжирования документов ..... 244
8.8.3. Основные поисковые системы ..... 250
8.8.4. Поисковая система Яndex ..... 251
8.8.5. Поисковая система Google ..... 255
8.8.6. Поисковая система Rambler ..... 260
**Контрольные вопросы** ..... 264
**ГЛОССАРИЙ** ..... 266
**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ** ..... 295



**М.Б.АБДУЖАППАРОВА**
**С.А.САДЧИКОВА,**

# ИНТЕРНЕТ СЕТИ И УСЛУГИ

**(Учебник)**

**Ташкент – «Aloqachi» – 2019**

Редактор: К. Маткурбанов
Тех. редактор: А. Тагаев
Художник: Б. Эсанов
Корректор: Ф. Тагаева
Компьютерная верстка: B.Berdimuradov

Изд. лиц. Ii №176. 11.06.2010.
Разрешено в печать: 15.11.2019.
Формат 60x84 1/16. Гарнитура «Times New Roman».
Усл. п.л. 19,25. Изд.п.л. 18,75. Тираж 60. Заказ № .