Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

В. А. Ганжа, В. В. Шиманский

КОМПЬЮТЕРНЫЕ СЕТИ. ВВЕДЕНИЕ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-40 04 01 «Информатика и технологии проектирования»

Минск БГУИР 2015

УДК 004.7(076)
ББК 32.973.202я73
Г19

Рецензенты:

кафедра информационных технологий
Республиканского института инновационных технологий
Белорусского национального технического университета
(протокол №3 от 17.11.2014 г.);

главный научный сотрудник государственного научного учреждения
«Объединенный институт проблем информатики Национальной
академии наук Беларуси», доктор технических наук,
доцент С. Ф. Липницкий

Ганжа, В. А.

Г19 Компьютерные сети. Введение : учеб.-метод. пособие / В. А. Ганжа, В. В. Шиманский. – Минск : БГУИР, 2015. – 155 с. : ил.

ISBN 978-985-543-145-0.

Разбираются проблемы построения, работы и обслуживания компьютерных сетей как необходимого элемента образования ИТ-специалиста. Учебно-методическое пособие содержит небольшую теоретическую часть в виде слайдов к лекциям и ряд лабораторных работ для практического исполнения, апробированных авторами на протяжении ряда лет на занятиях со студентами.

УДК 004.7(076)
ББК 32.973.202я73

ISBN 978-985-543-145-0

Содержание

Введение

Роль компьютерных сетей в наше время огромна. Это и работа в команде разъединённых территориально разработчиков. Это и хранение данных в сетевых хранилищах. Это, наконец, обычное человеческое общение – чат, электронная почта, живое on-line видеообщение партнёров и друзей. Рассмотрим кратко, что представляет из себя компьютерная сеть с технической точки зрения.

Создание компьютерных сетей требует решения ряда задач:

- адресация – выяснение, кому из абонентов предназначено сообщение;
- контроль доступа к среде – предотвращение конфликтных ситуаций, когда двое абонентов одновременно пытаются использовать одну и ту же линию;
- управление производительностью – сохранение работоспособности сети в случае её перегрузки сообщениями;
- своевременность доставки сообщений – это требование противоречит первым пунктам, но обеспечить своевременную доставку сообщения абоненту очень важно;
- отказоустойчивость – обеспечение работоспособности сети при отказе отдельных линий или отдельных узлов;
- безопасность – гарантия того, что абоненты, которым не предназначено сообщение, не смогут прочитать или исказить его.

В зависимости от сферы применения сети решению этих задач уделяется большее или меньшее внимание.

Создание больших сетей требует включения в сеть дополнительных узлов, осуществляющих маршрутизацию и ретрансляцию передаваемых данных. В зависимости от типа сети и стратегии коммутации такие узлы называются **коммутаторами** (свитч – switch) или **маршрутизаторами** (релеями).

В настоящий момент известны три стратегии коммутации [4] сетей:

- **сети с коммутацией сообщений**, когда сообщение передаётся целиком с возможным промежуточным хранением;
- **сети с коммутацией каналов**, когда сообщение передаётся целиком, но нигде по дороге не хранится и ограничения на время существования канала не вводятся (но может взиматься повременная тарифная оплата);
- **сети с коммутацией пакетов**, когда сообщение режется на пакеты небольшого размера и когда эти пакеты хранят-

ся на промежуточных узлах, но промежуточные узлы не пытаются собрать их в цельное сообщение.

Сети с коммутацией сообщений – наиболее давние и наиболее старые. Этот способ передачи сообщений уже использовался несколько тысячелетий назад. Это сеть эстафетных станций вдоль основных дорог древнего Рима, которые использовались для передачи военных донесений и приказов, позже эстафетные станции стали использоваться состоятельными римскими гражданами.

В России сеть ямских станций вдоль важнейших дорог просуществовала до XIX века. Это типичная сеть с коммутацией сообщений. Поначалу ямские станции использовались исключительно для государственного управления; позже через них разрешили пересылать корреспонденцию состоятельным гражданам, а потом уже адаптировали и для перевозки пассажиров. Ямские станции постепенно становились центрами сортировки сообщений.

Сеть ямских станций явилась прообразом структуры организации современной почты. А в XIX веке на базе такой сети возникла телеграфная сеть, сохранившая основные принципы почтовой сети. Роль перегонов между станциями стали выполнять телеграфные линии, а сами станции заменили телеграфными узлами. Маршрутизация сообщений (телеграмм) осуществлялась вручную телеграфистами-операторами.

Современная электронная почта – типичная почтовая сеть с коммутацией сообщений поверх глобальной компьютерной сети.

Сети с коммутацией каналов первоначально использовались только для передачи человеческого голоса, а потом стали называться телефонными сетями. Телефонная сеть – крупнейшая сетевая инфраструктура, и современные сети передачи данных существуют и сотрудничают с такими сетями. Сеть с коммутацией каналов через сеть промежуточных телефонных станций, называемых АТС, осуществляет прямое соединение телефонных аппаратов абонентов.

Сети с коммутацией пакетов предполагают предварительное расчленение сообщения на небольшие доли, каждая доля снабжается конечным адресом абонента и путешествует по сети самостоятельно. Эти доли могут перемещатся по сети по разным маршрутам. Обратная операция сборки сообщения из долек осуществляется на конечном пункте у абонента. В промежуточных пунктах эти дольки сортируются по своим маршрутам. Соответствующее

оборудование, осуществляющее эту операцию, называется маршрутизатором.

Такой сложный метод, как **коммутация пакетов,** применяется, во-первых, для использования максимальной пропускной способности существующих физических линий связи, во-вторых, в таких сетях отсутствует этап соединения и состояние «занято». Сеть всегда готова передать данные пользователя. В-третьих, в сети с коммутацией пакетов становятся возможными сервисы, которых не может быть в сетях первых двух типов.

Ясно, что такие сложные сети с предварительным расчленением сообщения, а потом с его окончательной сборкой в пункте назначения требуют очень сложных протоколов для обеспечения надёжной работы. Поэтому сети с коммутацией пакетов получили распространение только в наши дни, при высоком уровне развития вычислительной техники.

В связи с этим большая часть данного учебно-методического пособия будет посвящена описанию сетей с коммутацией пакетов.

1 Теоретическая часть

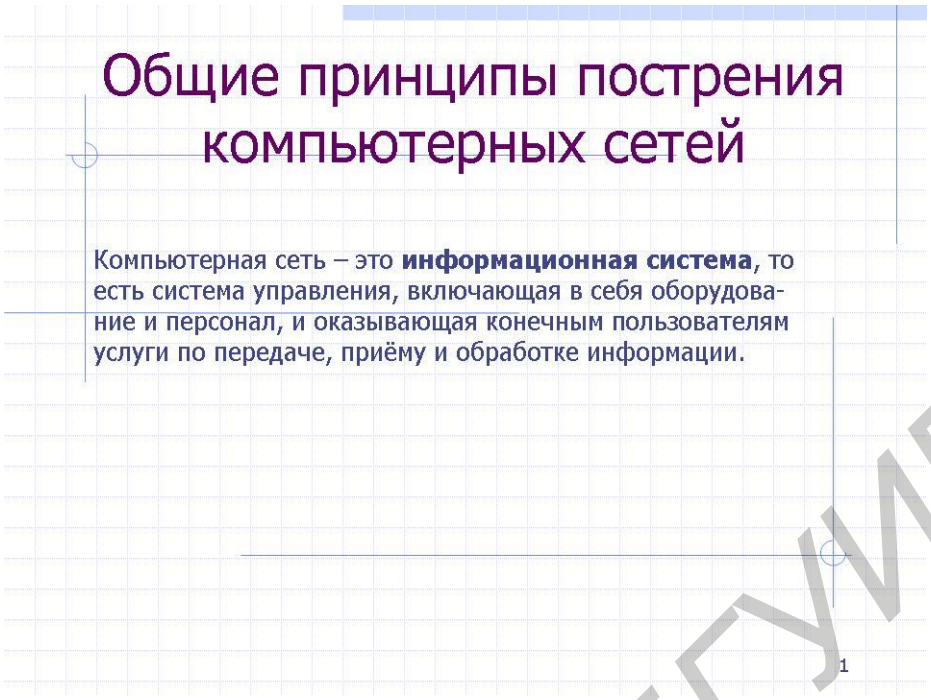
1.1 Лекция. Компьютерные сети. Сети с коммутацией каналов и с коммутацией пакетов

Компьютерные сети появились недавно и они унаследовали много полезных свойств от других, более старых и распространённых телекоммуникационных сетей, например телефонных. Со своей стороны компьютерные сети привнесли в телекоммуникационный мир новые свойства – они сделали доступными огромные объёмы информации, созданные цивилизацией за несколько тысячелетий.

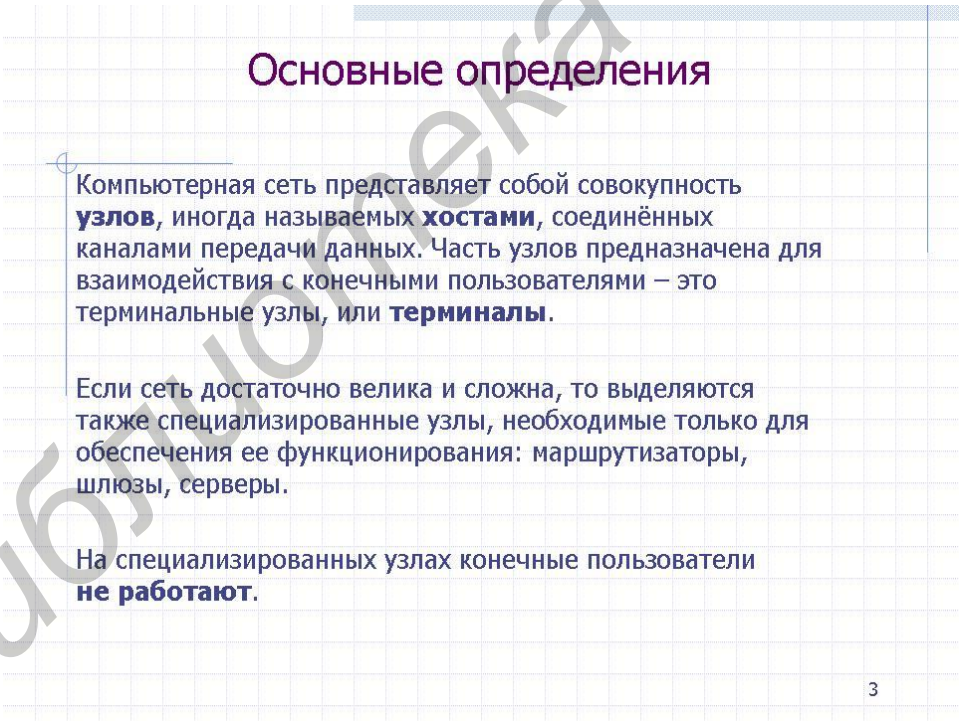
Существуют общие принципы построения компьютерных сетей, зная которые вы сможете разбираться с конкретной сетевой технологией. Знание принципов позволит систематизировать эти сведения, связать их друг с другом и тем самым использовать осознанно и эффективно.

Здесь мы рассмотрим понятия сетевых технологий, коммутации и маршрутизации, использование общей передающей среды. Познакомимся с общими подходами, применяющимися при адресации узлов сети и выборе топологии сети.

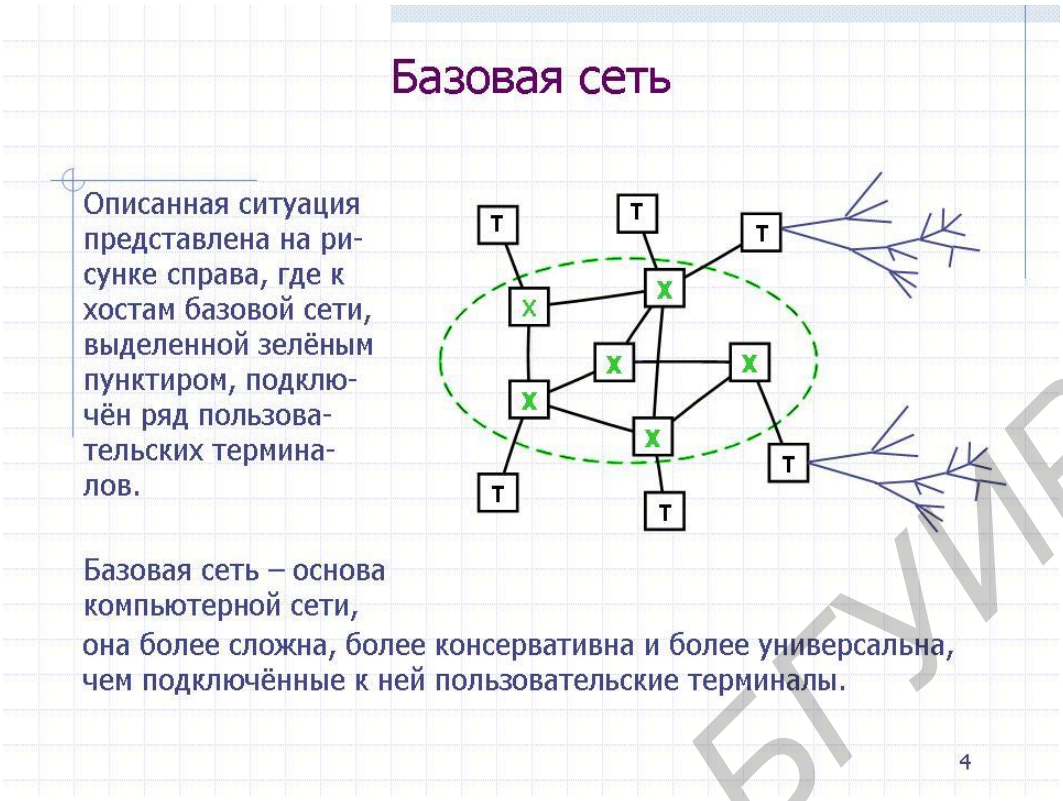
Компьютерные сети – это сети с коммутацией пакетов. Бесспорна эффективность таких сетей, с одной стороны, но с другой стороны, они сложны в управлении. Как следствие этой сложности возник стек протоколов для обмена данными в сетях с коммутацией пакетов. Существует несколько наборов протоколов для управления такими сетями: семиуровневая классическая европейская модель OSI; реальная американская модель TCP/IP; стеки NetBiOS, IPX/SPX.



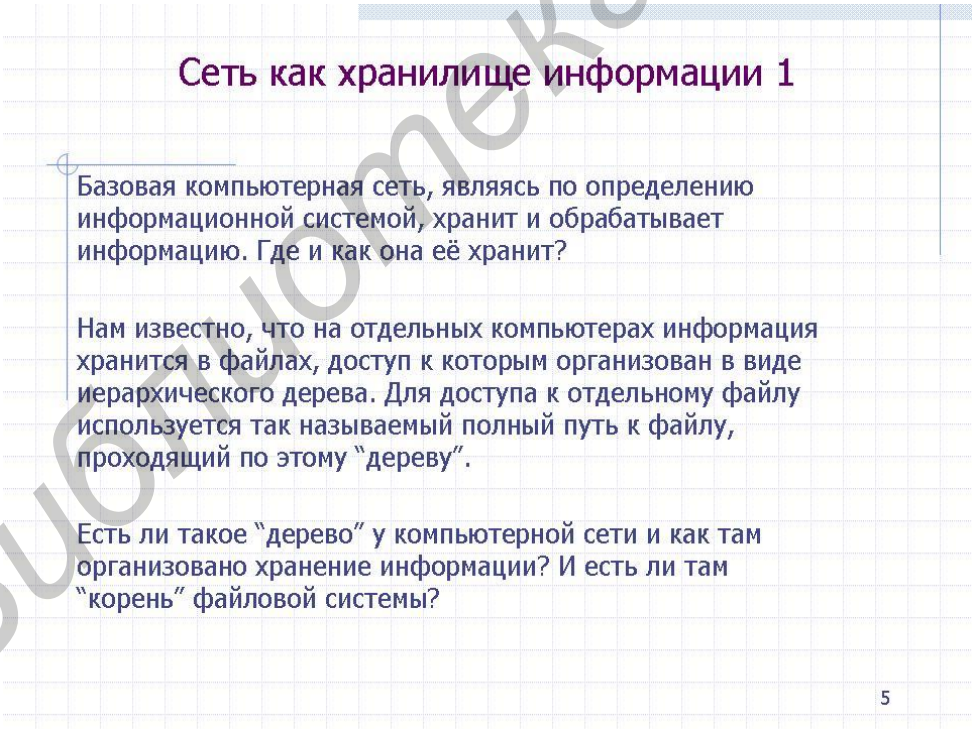
Слайд 1. Компьютерная сеть – большой гетерогенный комплекс аппаратуры, программного обеспечения и обслуживающего персонала.



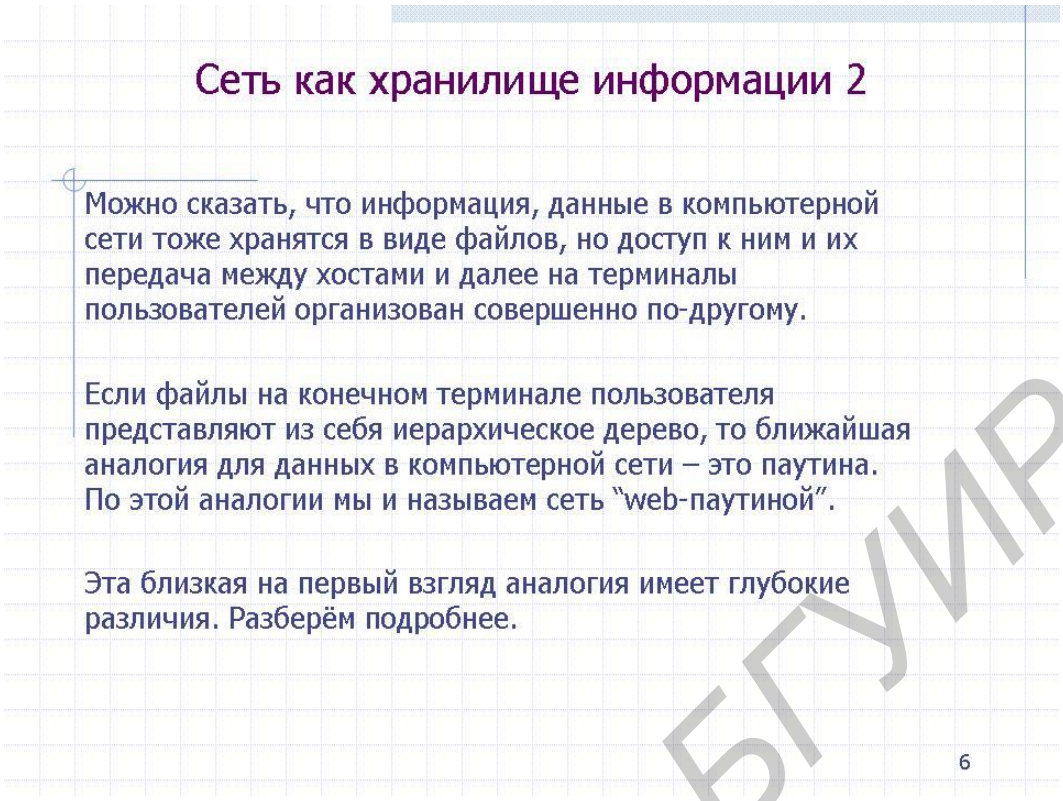
Слайд 2. Для работы и функционирования компьютерной сети необходимо специальное оборудование и программное обеспечение.



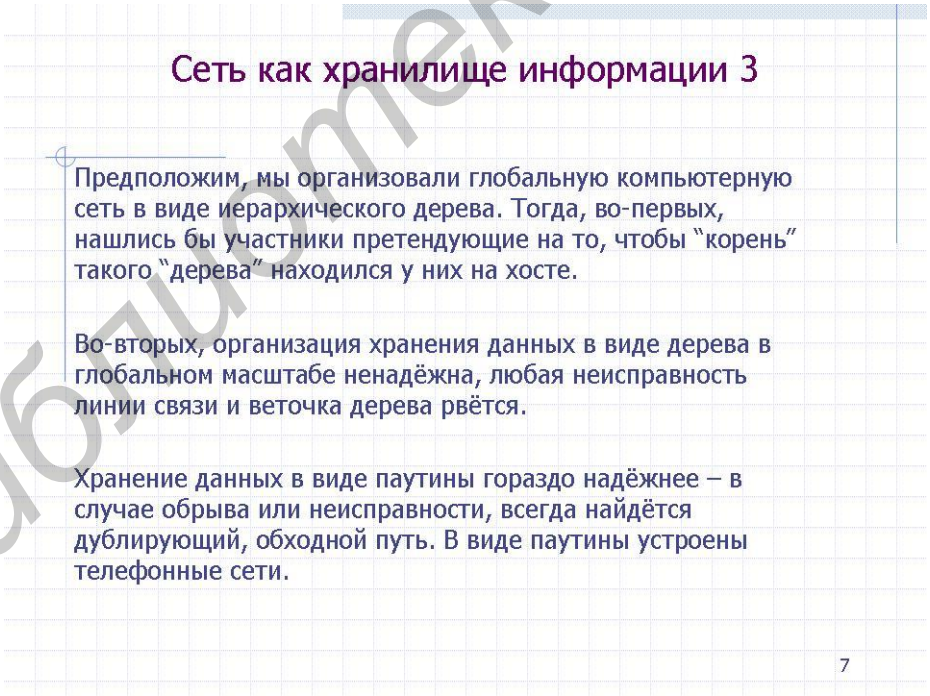
Слайд 3. Специализация различных компонентов компьютерной сети.



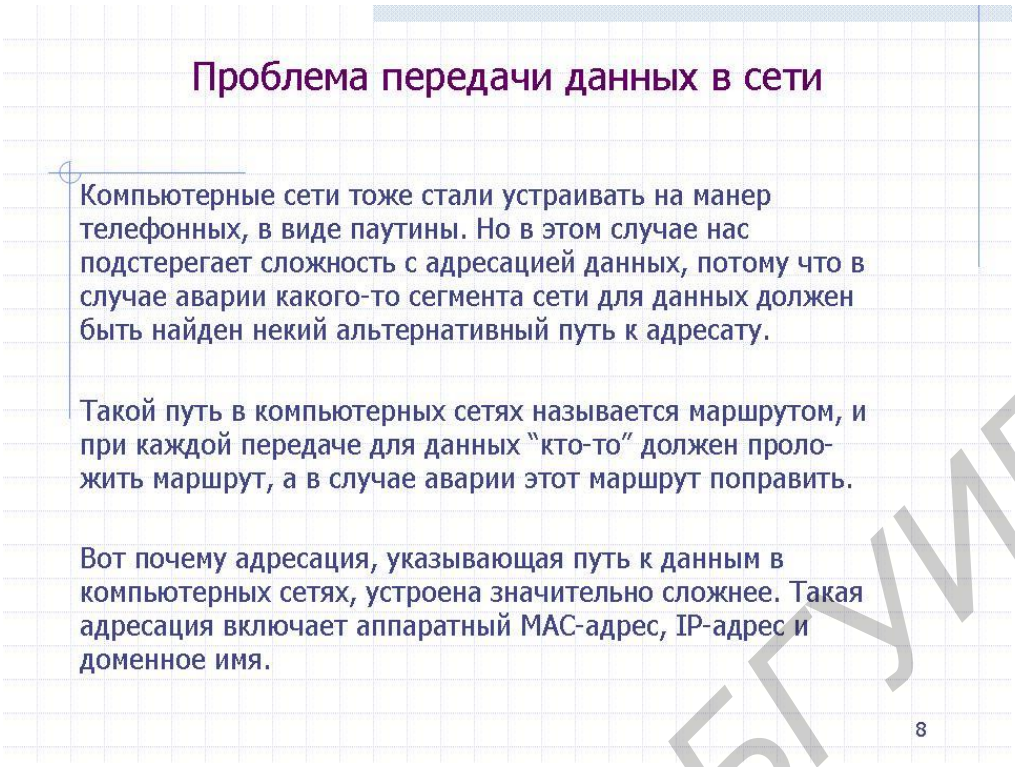
Слайд 4. Разный подход к хранению информации на локальном компьютере и в глобальной сети.



Слайд 5. Сохранение и доступ к информации в сети в виде паутины повышает надёжность доступа в случае отказа отдельных звеньев.

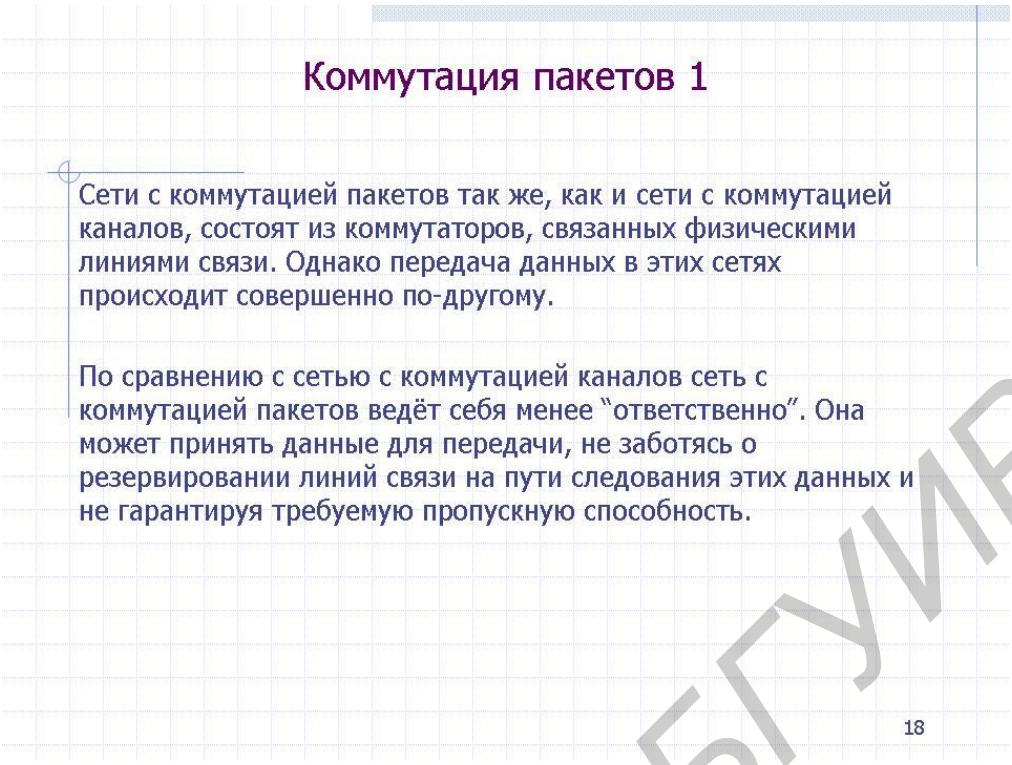


Слайд 6. Доступ к информационной «паутине» сложнее, чем к иерархической файловой системе.

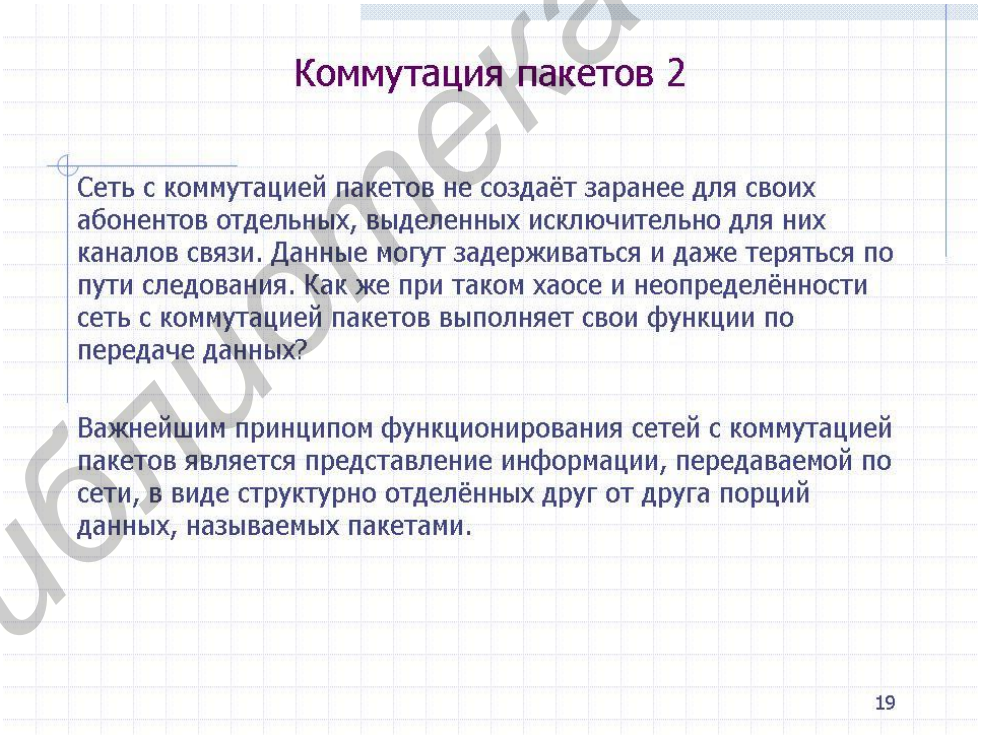


Слайд 7. Для адресации к информационным ресурсам сети необходимо несколько адресов: MAC-адрес и IP-адрес.

Слайд 8. Три стратегии передачи сообщений в коммуникационных сетях.



Слайд 9. Надёжный, но сложный метод передачи данных с коммутацией пакетов.

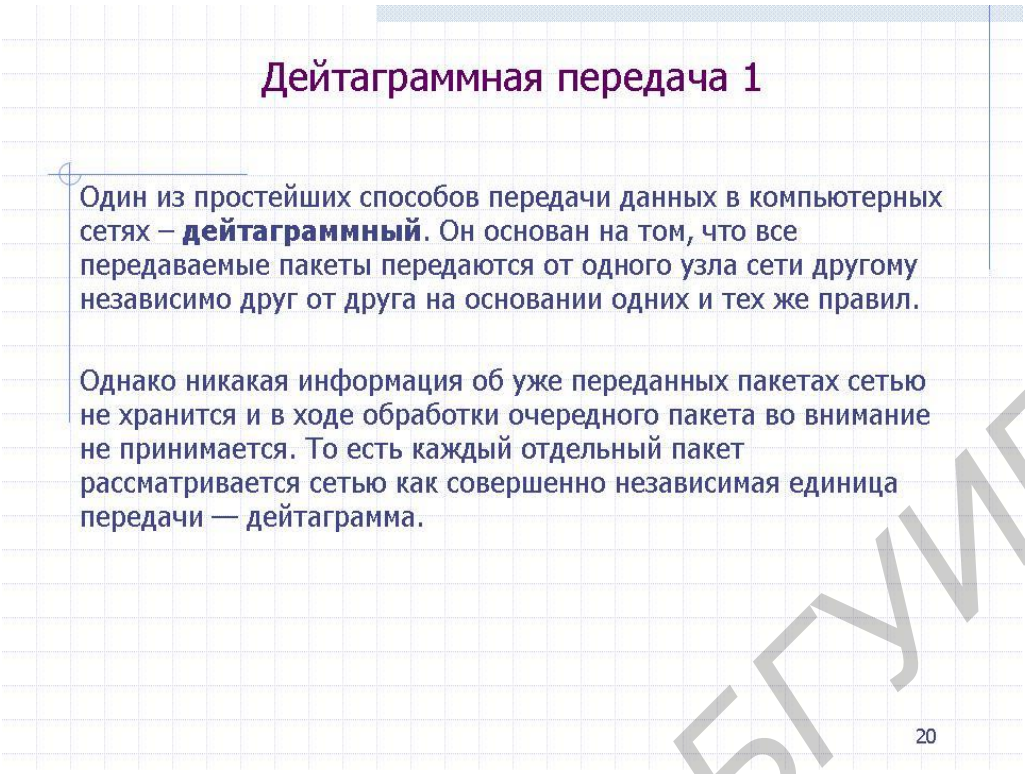


Слайд 10. Данные пользователя дробятся на дольки перед отправкой в сеть. Каждая долька добирается к партнёру самостоятельно.

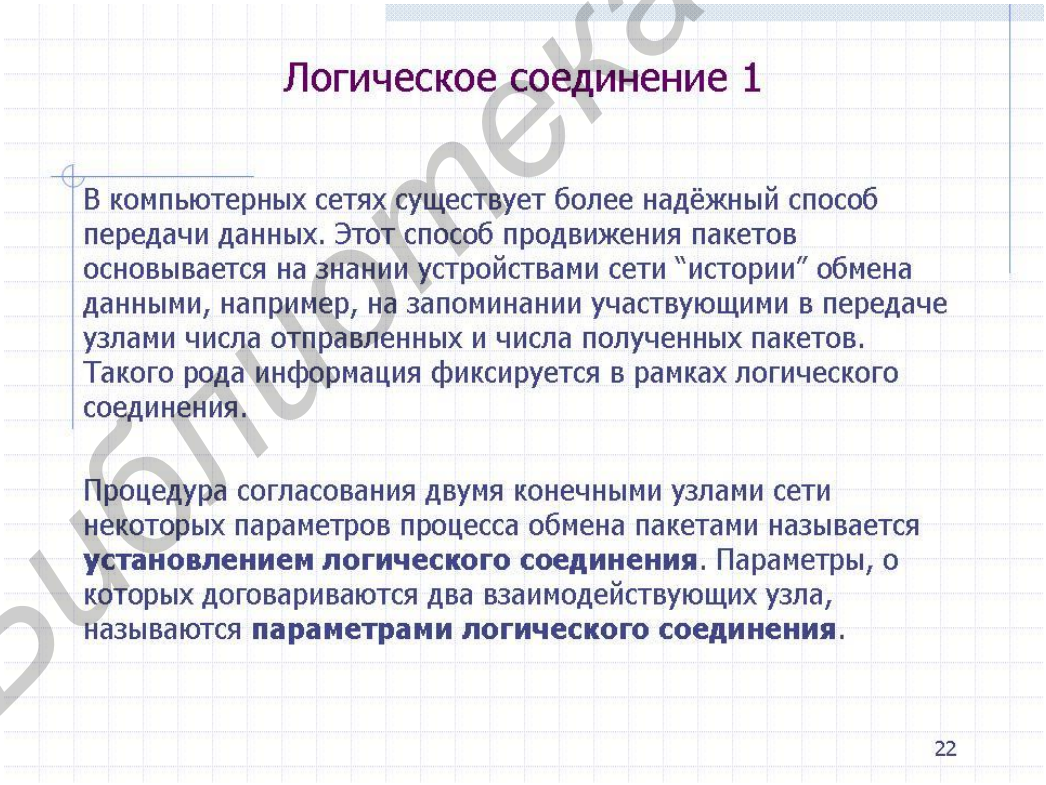
Слайд 11. Дробление данных на части перед отправкой их в сеть и обратная их сборка на конечном пункте – на компьютере партнёра.

Коммутация каналов и пакетов – сравнение [5]

	Коммутация каналов	**Коммутация пакетов**
1	Необходимо предварительно устанавливать соединение.	Отсутствует этап установления соединения (дейтаграммный способ).
2	Адрес требуется только на этапе установления соединения.	Адрес и другая служебная информация передаются с каждым пакетом.
3	Сеть может отказать абоненту в установлении соединения.	Сеть всегда готова принять данные от абонента.
4	Гарантированная пропускная способность (полоса пропускания) для взаимодействующих абонентов.	Пропускная способность сети для абонентов неизвестна, задержки передачи носят случайный характер.
5	Трафик реального времени передаётся без задержек.	Ресурсы сети используются эффективно при передаче пульсирующего трафика.
6	Высокая надёжность передачи данных.	Возможны потери данных из-за переполнения буферов.
7	Нерациональное использование пропускной способности каналов, снижающее общую эффективность сети.	Автоматическое динамическое распределение пропускной способности физического канала между абонентами.



Слайд 12. Быстрый, но не очень надёжный способ передачи данных – дейтаграммный.



Слайд 13. Логическое соединение – основа надёжной передачи данных в компьютерных сетях.

Архитектура компьютерных сетей 2

Стандартизация архитектуры компьютерной сети может быть описана моделью взаимодействия открытых систем **OSI** (Open System Interconnection, OSI).

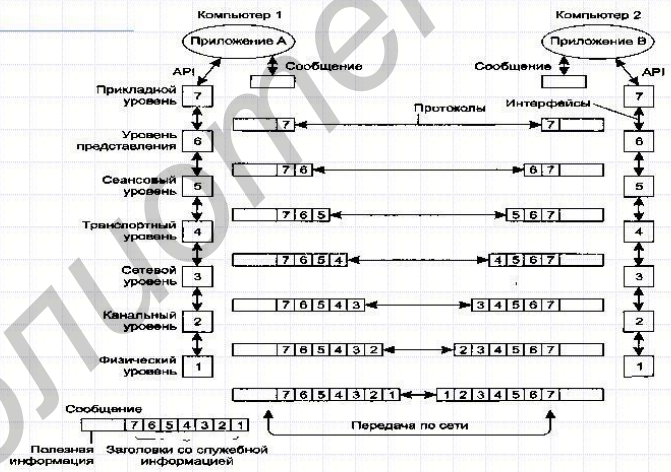
Модель OSI является международным стандартом и определяет способ взаимодействия узлов "по вертикали", с помощью ряда протоколов, которые функционально привязываются к семи базовым концепциям, называемым уровнями.

Эти уровни образуют иерархию, известную как стек протоколов, где каждый вышестоящий уровень использует нижестоящий в качестве удобного инструмента для решения своих задач.

30

Слайд 14. OSI – набор протоколов для обеспечения работы сетей, использующих стратегию «коммутация пакетов».

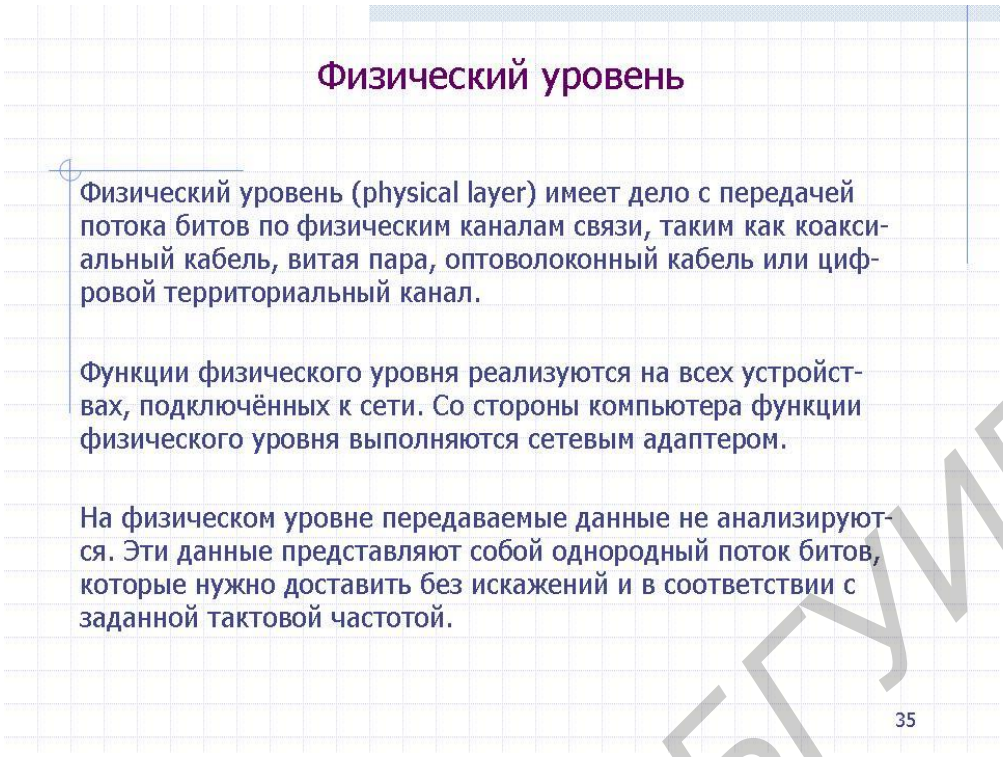
Разделение модели OSI на 7 уровней



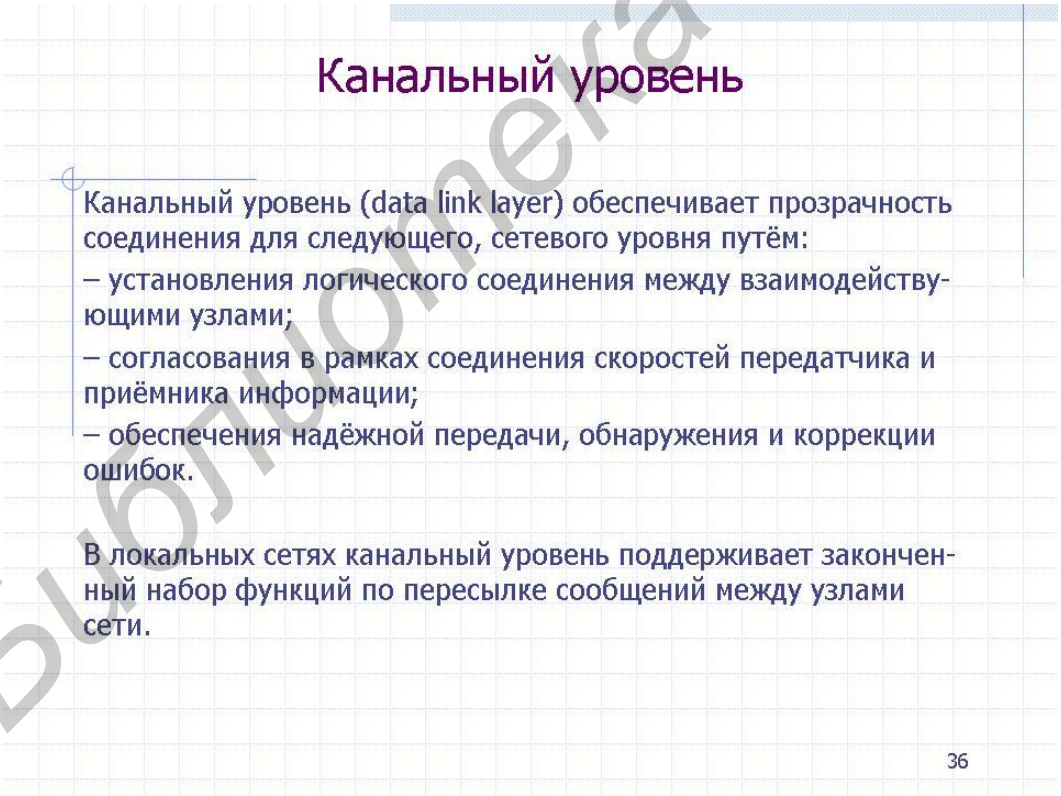
Модель взаимодействия открытых систем OSI

29

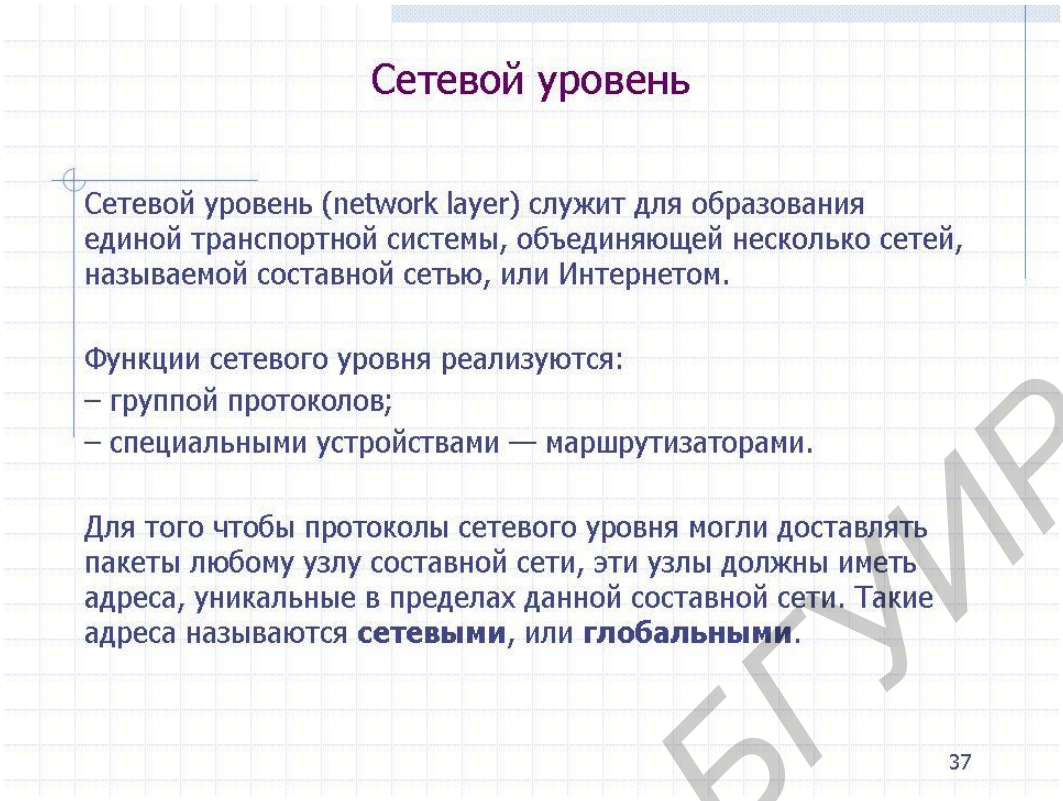
Слайд 15. Схема инкапсуляции пакетов. При продвижении пакета вниз, к физическому уровню, он обрастает служебной информацией.



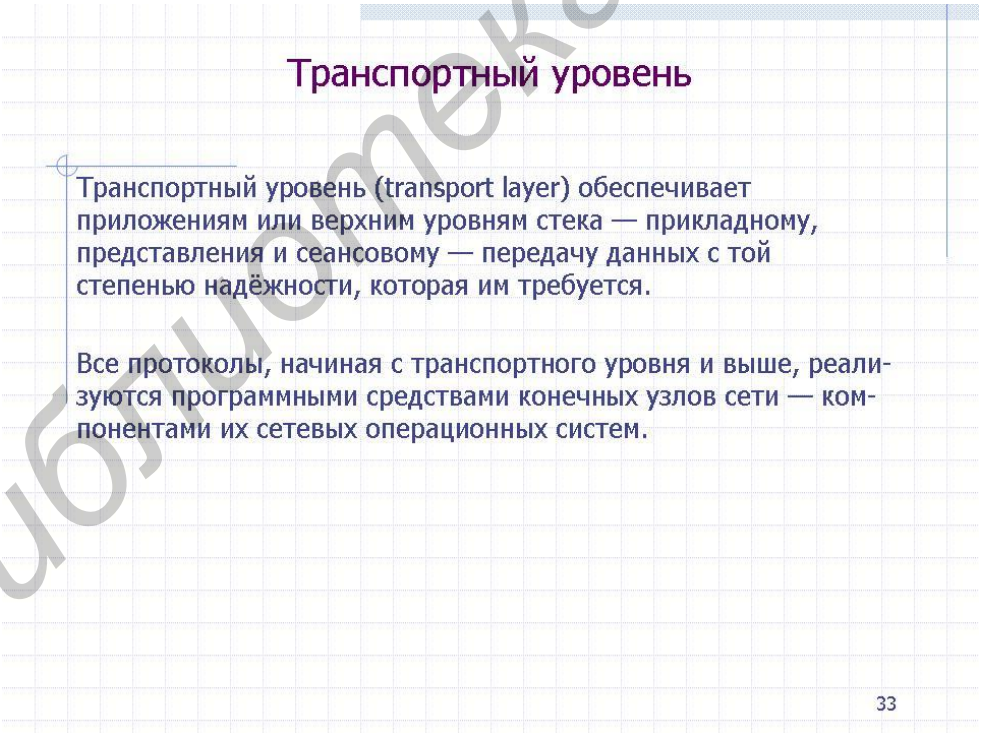
Слайд 16. Протоколы физического уровня ответственны только за передачу потока битов через среду передачи данных.



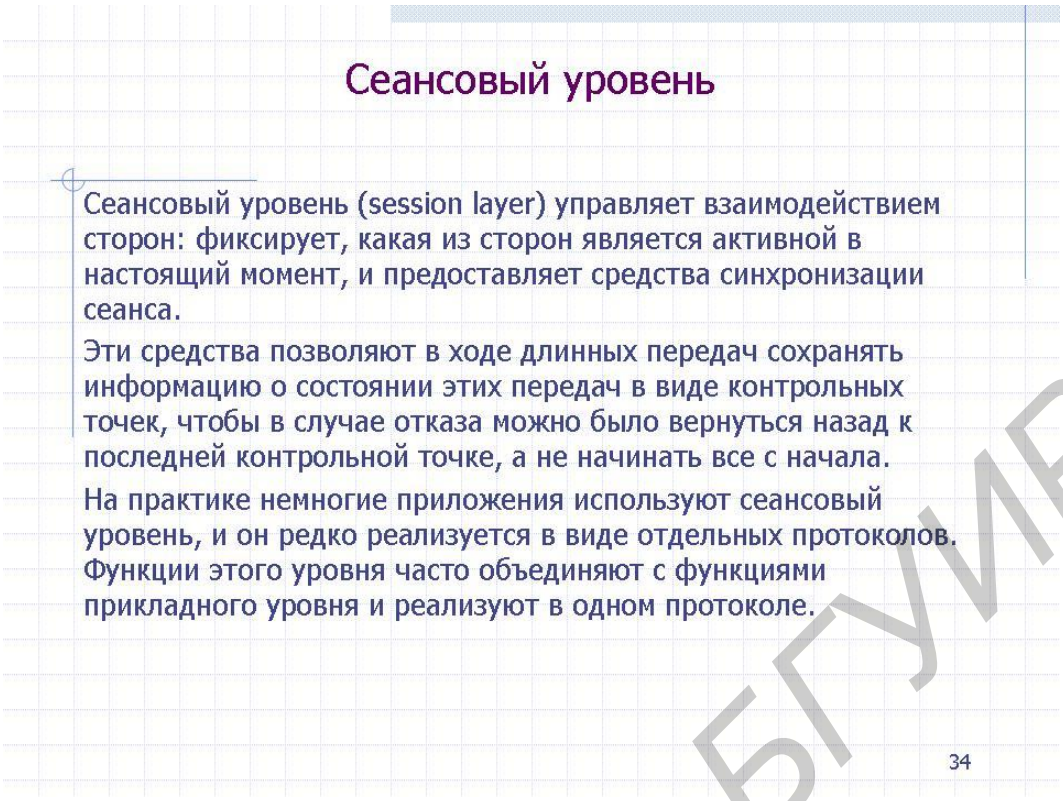
Слайд 17. Один из самых сложных уровней модели OSI. Он даже расщепляется на два подуровня.



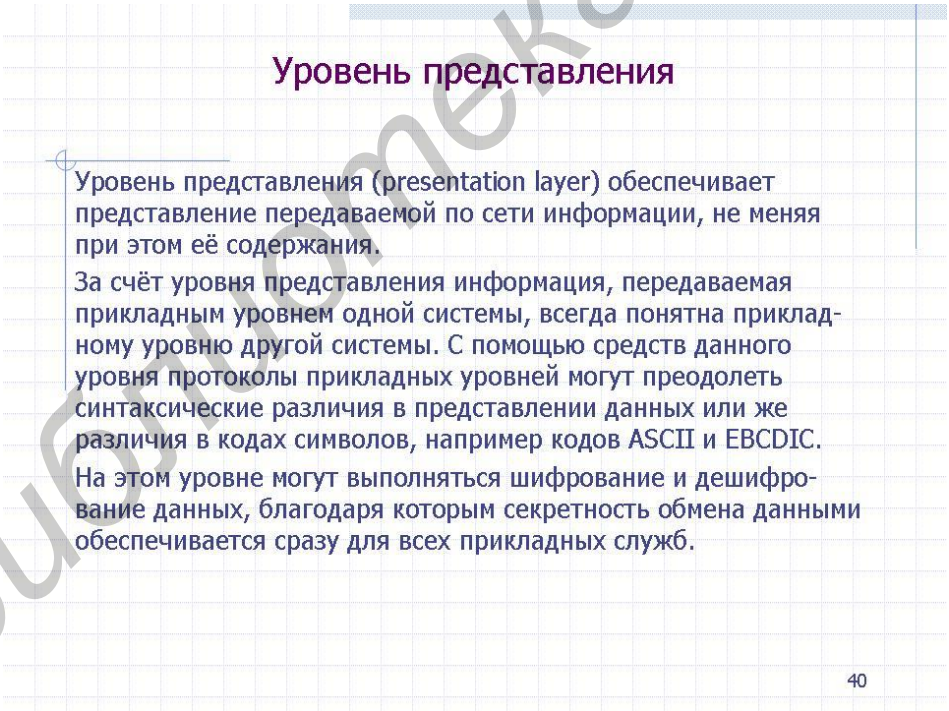
Слайд 18. Сетевой уровень объединяет глобальную сеть. Здесь пакеты направляются по необходимым маршрутам.



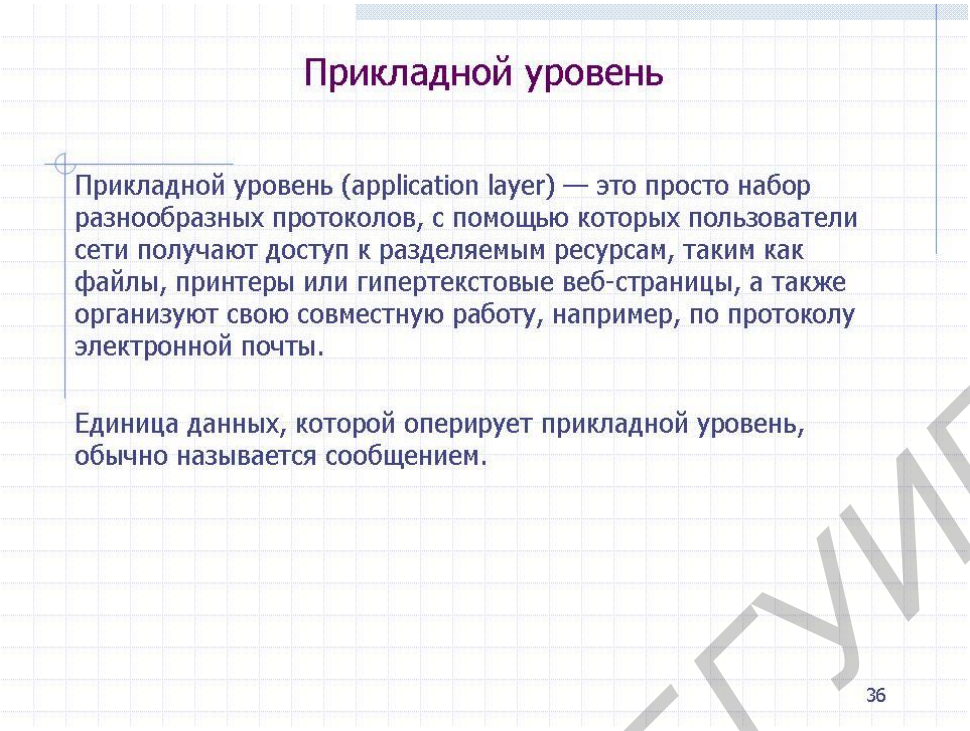
Слайд 19. Транспортный уровень отслеживает целостность данных и передаёт их различным приложениям операционной системы.



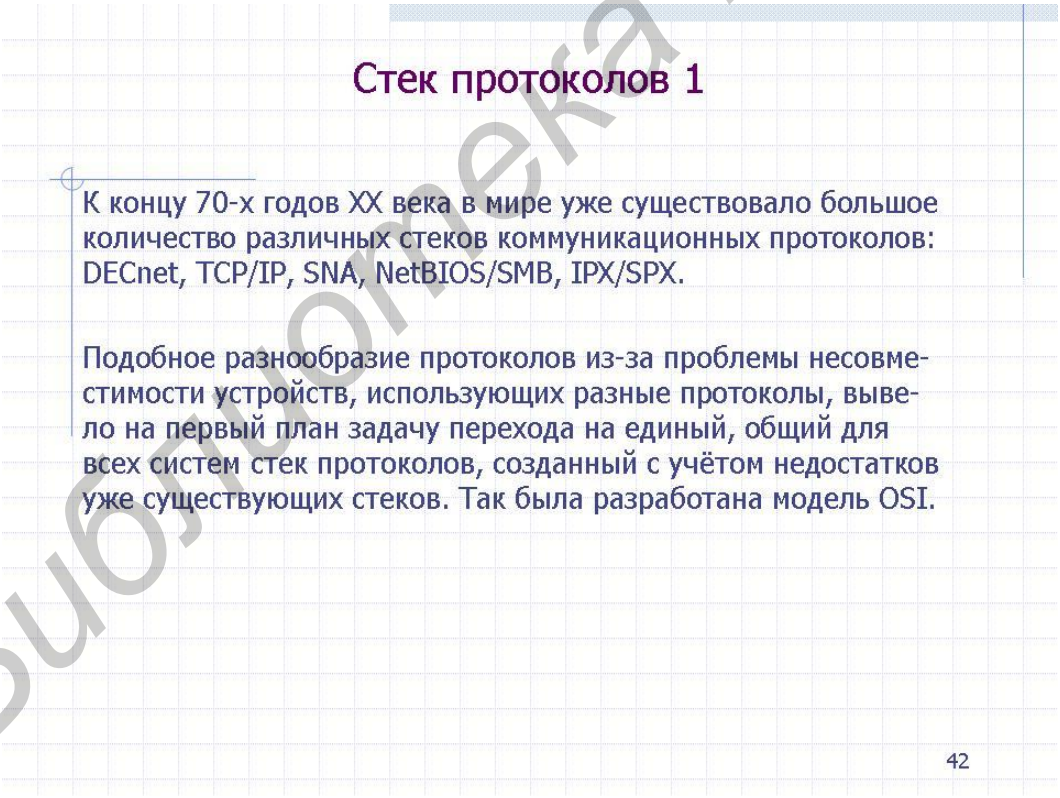
Слайд 20. Этот уровень малофункционален и в стеке TCP/IP объединён с прикладным уровнем.



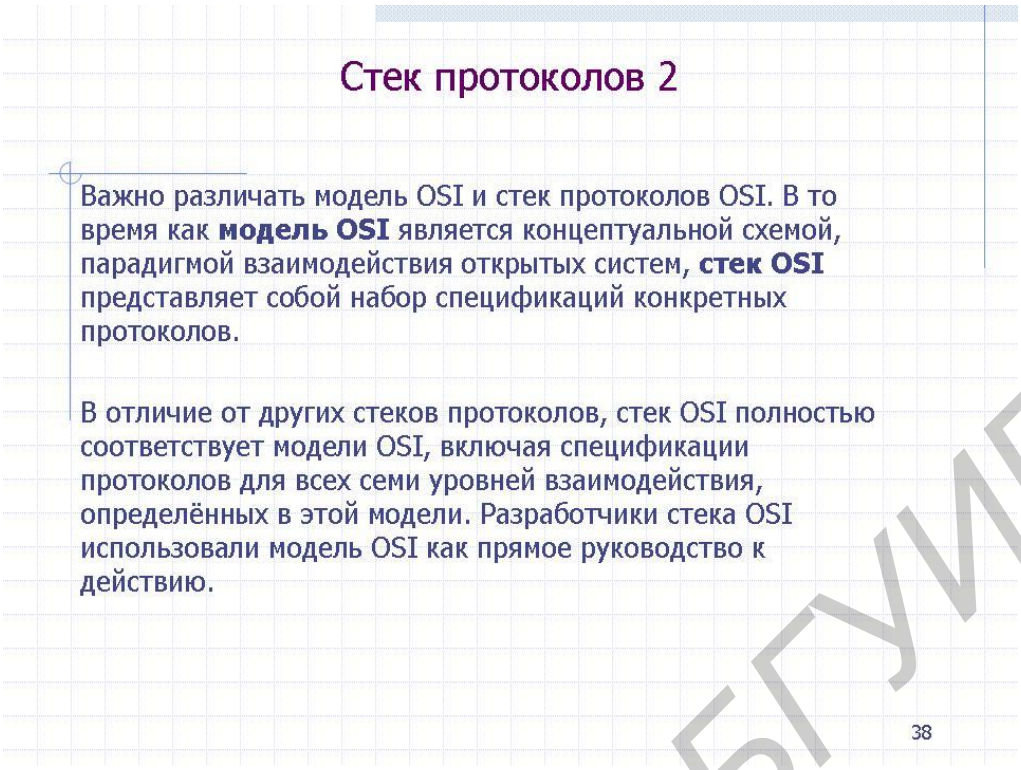
Слайд 21. Этот уровень беден протоколами и тоже объединён с прикладным уровнем.



Слайд 22. На прикладном уровне работают процессы и приложения многозадачной операционной системы.



Слайд 23. Практическое использование в компьютерных сетях получил стек протоколов TCP/IP.



Слайд 24. Стек модели OSI красив и логически совершенен, но особого распространения и практической реализации в компьютерных сетях не получил.

Заключение

Компьютерные сети стали логическим результатом эволюции компьютерных и телекоммуникационных технологий. Они являются частным случаем распределённых компьютерных систем и могут рассматриваться как средство передачи информации на большие расстояния.

Принято классифицировать сети по территориальному признаку и различать **глобальные** и **локальные** сети.

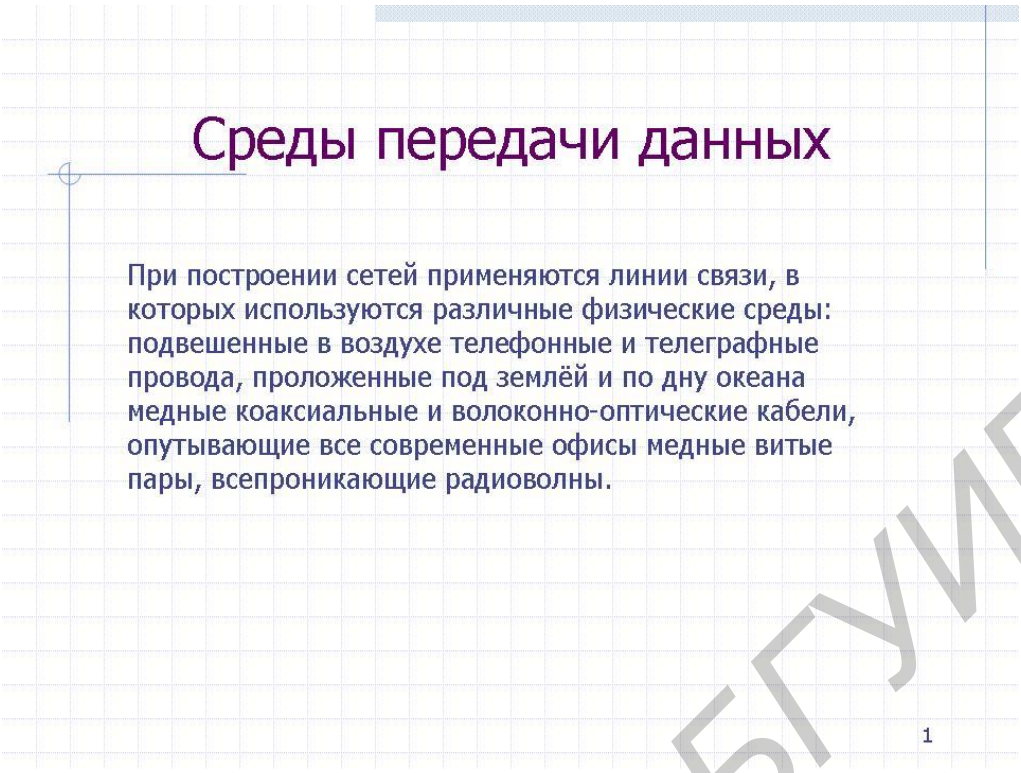
Локальные сети ограничены расстояниями в несколько километров; в них используются высококачественные линии связи, применяющие более простые методы передачи данных, чем в глобальных сетях, этим достигаются высокие скорости обмена данными.

Глобальные сети объединяют компьютеры в регионах на расстоянии тысяч километров. Глобальные компьютерные сети многое унаследовали от телефонных сетей, в том числе существующие и не очень качественные линии связи, это привело к низким скоростям передачи данных и ограниченному набору услуг: передача файлов и электронная почта.

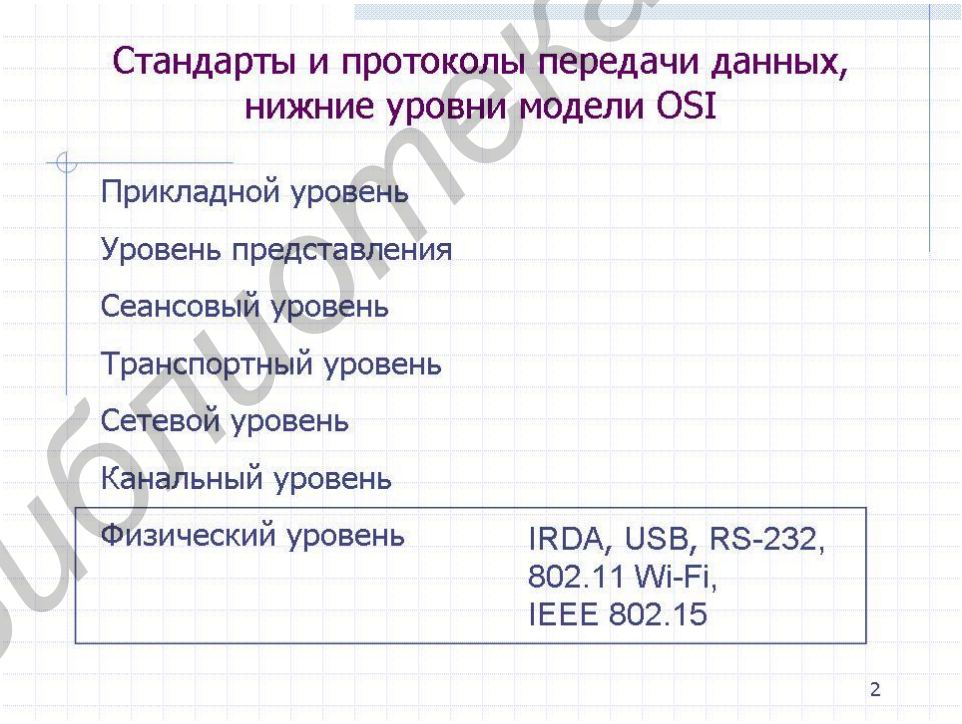
1.2 Лекция. Среды передачи данных

Компьютерные сети для передачи данных используют линии связи, которые отличаются физической средой. Передача данных – это процесс обмена информацией в двоичной форме между двумя и более точками. Этот процесс часто еще называют цифровой связью, так как на сегодняшний день большая часть информации передается в цифровой форме и циркулирует между компьютерами, между компьютерами и терминалами, принтерами, а также другими периферийными устройствами [8]. Данные могут быть представлены в простейшей форме, двоичными цифрами 1 и 0, или в более сложной, например символами клавиатуры. В любом случае цифры или символы представляют информацию.

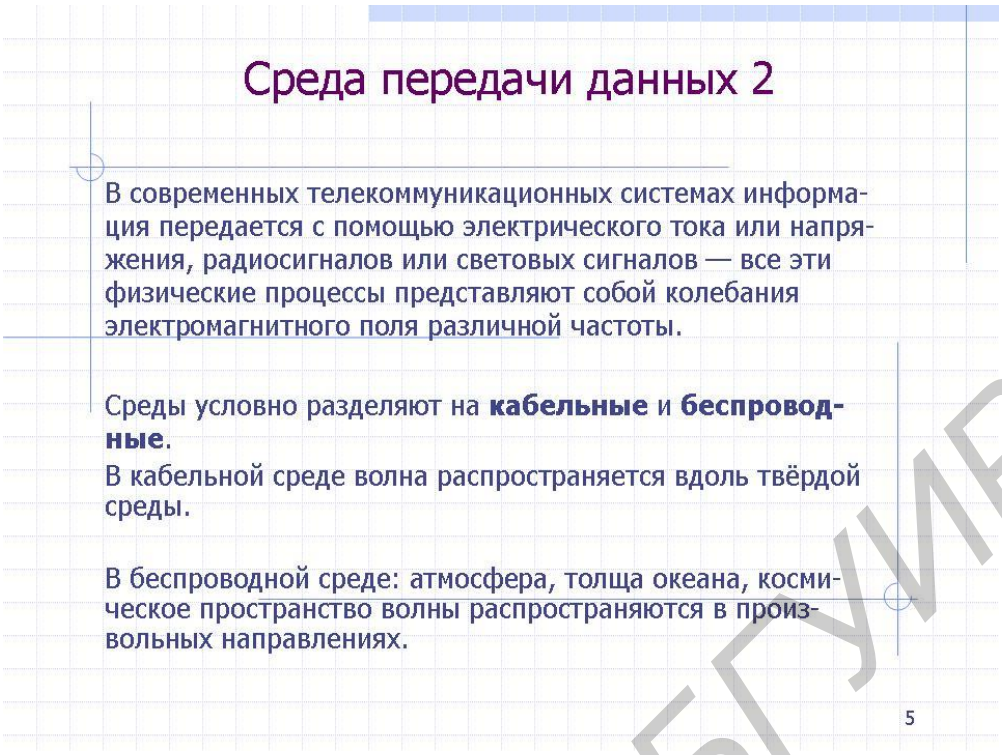
Здесь мы рассмотрим кабельные, или проводные, среды и беспроводную среду. Вспомним шкалу электромагнитных волн и позиционируем на ней различные источники информации: радио, телевидение, радары, оптические сигналы. Рассмотрим преимущества и недостатки спутниковой связи, геостационарных спутников. Узнаем, чем характеризуют качество обычного провода, витой пары, коаксиального кабеля, оптоволоконного кабеля. Разберём понятие полосы пропускания линии связи и научимся с помощью формулы Шеннона оценивать предельную скорость передачи данных через такую линию связи. Вкратце коснёмся мало исследованного вопроса передачи данных через гидросреду.



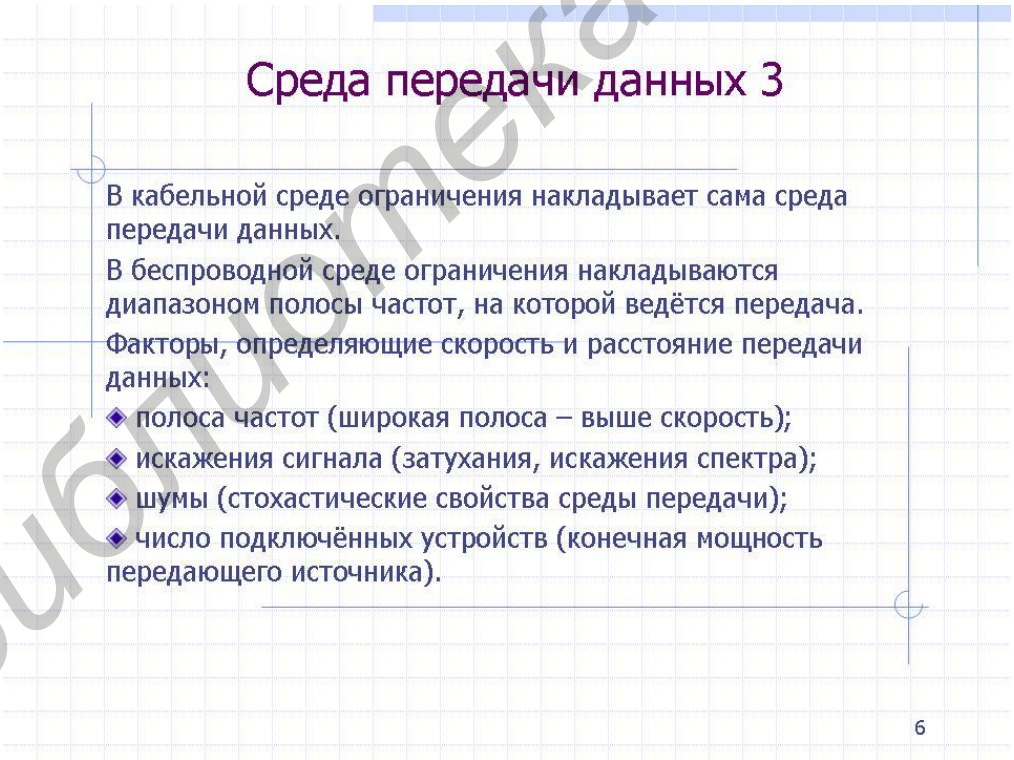
Слайд 1. Для передачи информации в компьютерных сетях может использоваться самая разная физическая среда.



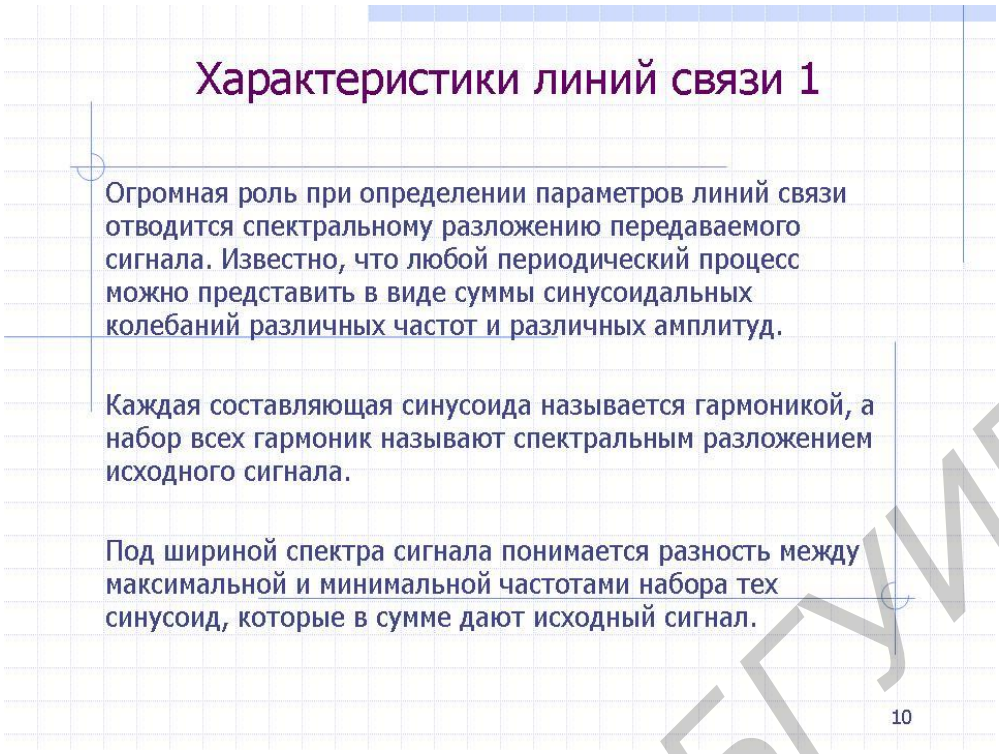
Слайд 2. Плоскость всех вопросов использования среды передачи данных относится к физическому уровню.



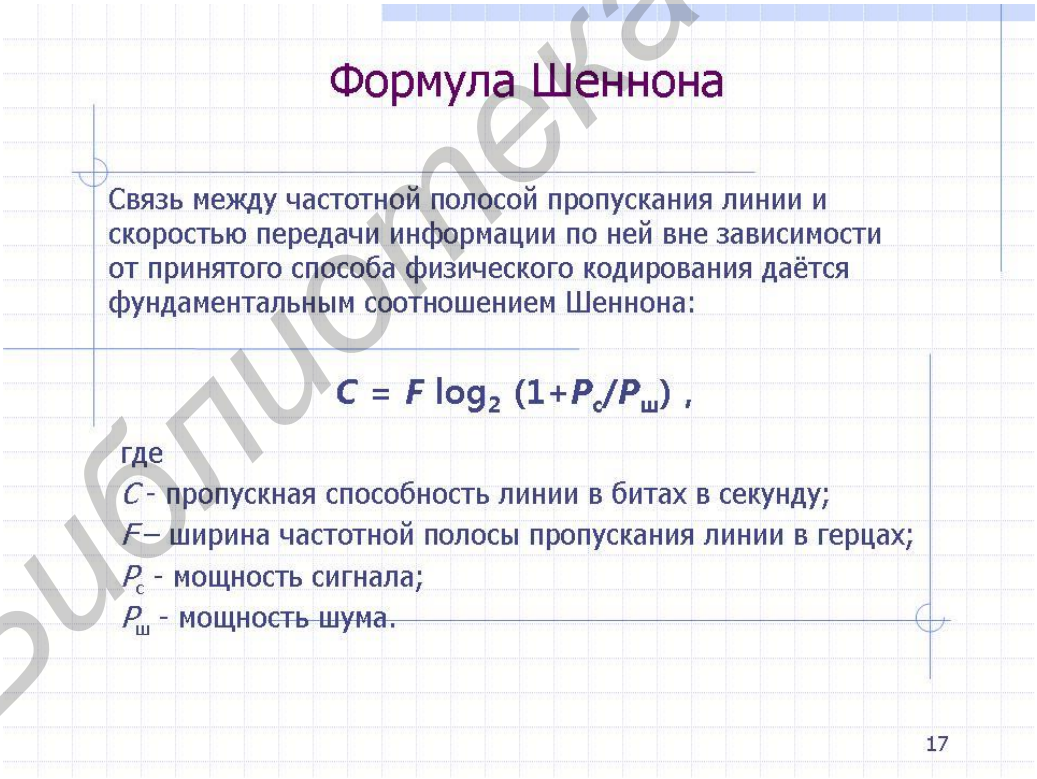
Слайд 3. Все среды передачи информации можно условно разделить на кабельные и беспроводные.



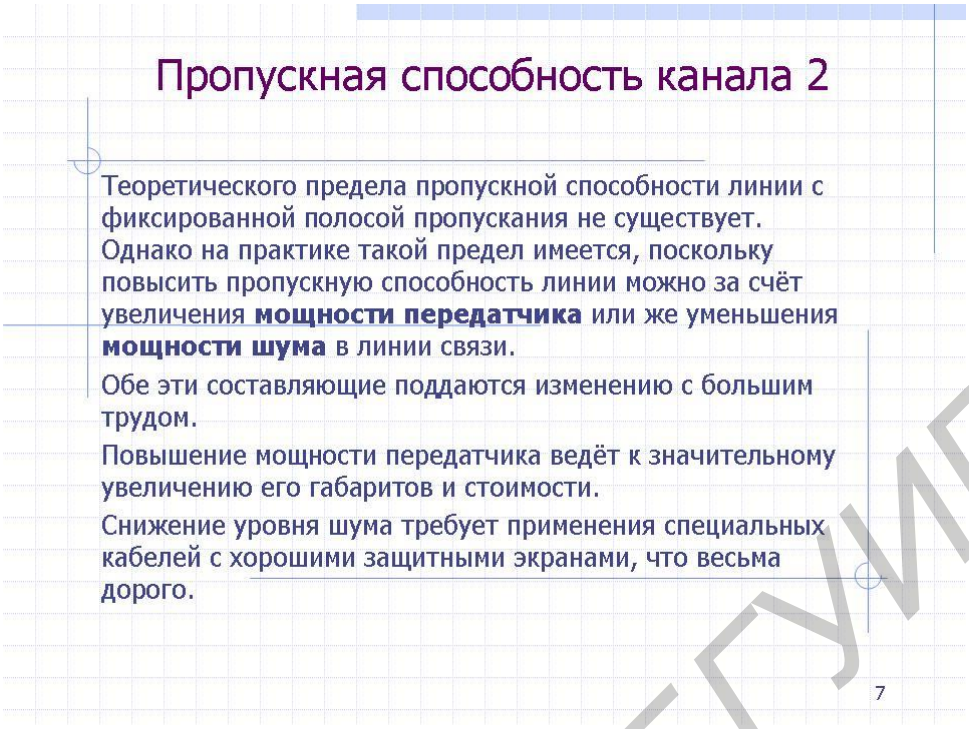
Слайд 4. Основное влияние на скорость передачи информации оказывает полоса частот пропускания сигнала и шумы.



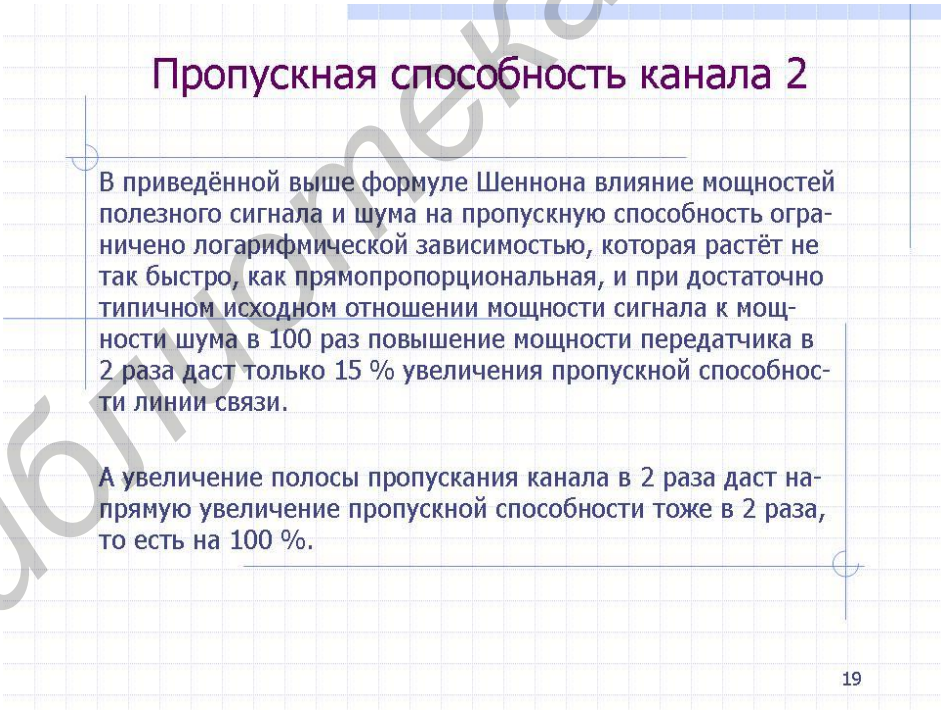
Слайд 5. Полоса частот пропускания сигнала, к сожалению, не всегда имеет плоскую прямоугольную форму.



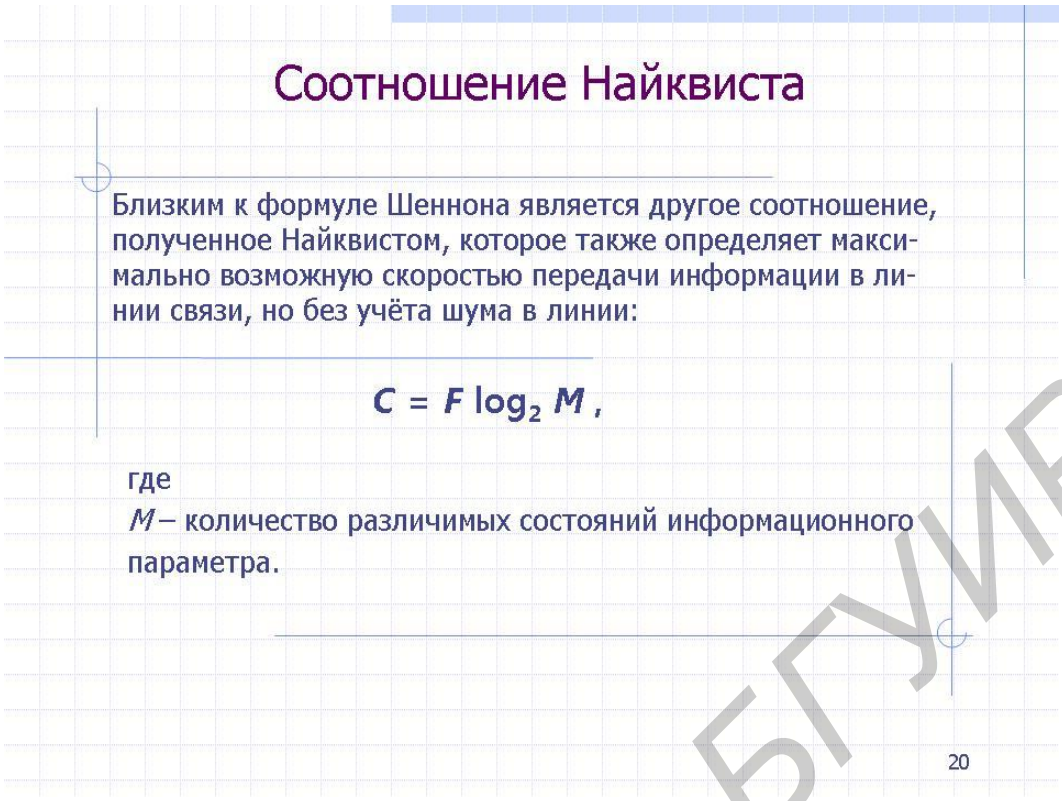
Слайд 6. Фундаментальное соотношение Шеннона для предельной скорости передачи информации в канале связи в *битах в секунду*.



Слайд 7. В реальной линии связи невозможно достигнуть предельной скорости, предписанной в фундаментальном соотношении Шеннона.



Слайд 8. Ключ к росту скорости передачи данных – увеличение полосы частот пропускания линии связи.



Слайд 9. Упрощённая формула Найквиста для скорости передачи информации, хорошо работающая на практике.

Слайд 10. Шкала электромагнитных волн применительно к беспроводным средам передачи данных.

Свойства кабельной среды

Кабельные среды. Качество передачи существенно зависит от расстояния передачи.

Характеристики двухточечных каналов связи на основе кабельных сред

	Полоса (Герц)	Затухание (дБ/км)	задержка (мкс/км)	расстояние (км)
телеф. каб.	0 - 3500	0,2	50	2
витая пара	$0 - 10^6$	3	5	2
коакс. кабель	$0 - 10^9$	7	4	1 – 9
оптоволокно	$10^{14} - 10^{15}$	0,2	5	40

11

Слайд 11. Основные характеристики кабельной среды: полоса частот пропускания сигнала и затухание сигнала в децибелах на 1 километр.

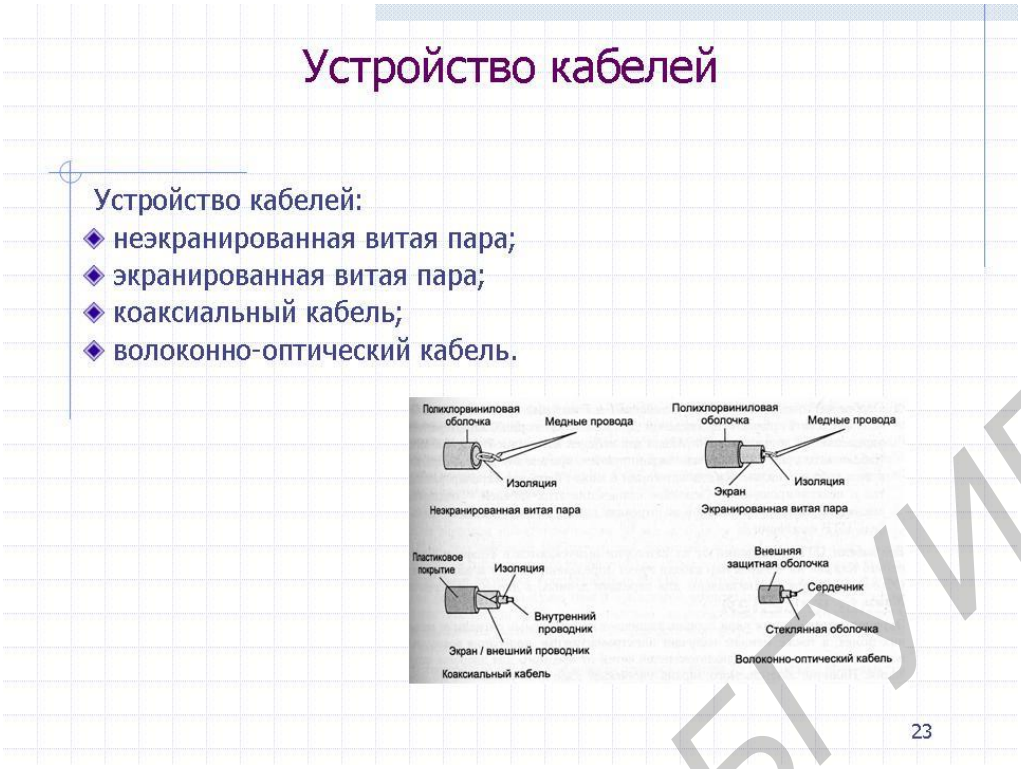
Типы сред передачи данных

- воздушные линии связи;
- кабельные линии связи;
- волоконно-оптические линии связи;
- радиоканалы наземной и спутниковой связи.

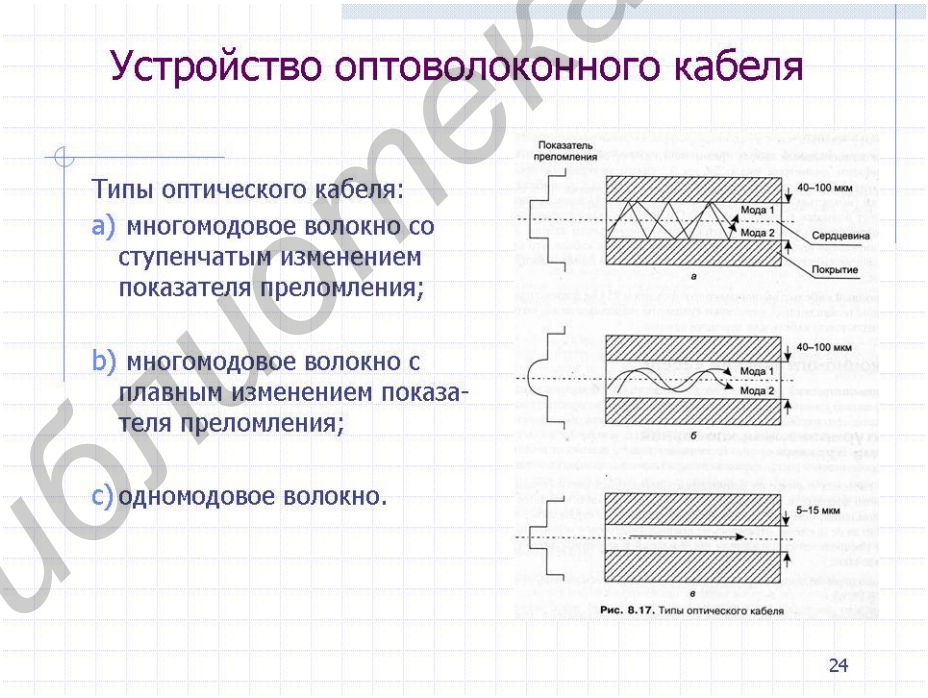
Рис. 8.2. Типы сред передачи данных

12

Слайд 12. Среды передачи данных.



Слайд 13. Экранированная витая пара с маленьким шагом навивки приближается по характеристикам к коаксиальному кабелю.

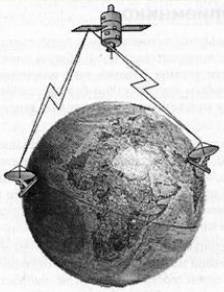


Слайд 14. Оптоволоконный кабель пока ещё дорог и требует сложной аппаратуры сопряжения с электронными оконечными устройствами.

Спутниковые системы 1

Частотные диапазоны спутниковой связи

Диапазон	Нисходящая частота, ГГц	Восходящая частота, ГГц
L	1,5	1,6
S	1,9	2,2
C	3,7-4,2	5,925-6,425
Ku	11,7-12,2	14,0-14,5
Ka	17,7-21,7	27,5-30,5



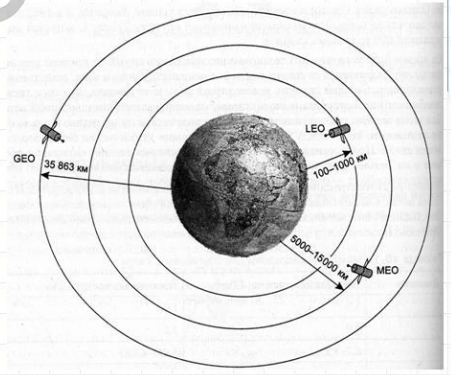
Спутник как отражатель сигнала

17

Слайд 15. Частотные диапазоны связи со спутником привязываются к окнам прозрачности атмосферы.

Типы орбит спутника

- GEO геостационарная орбита (35 863 км);
- MEO средневысотная орбита (5000 -15 000 км);
- LEO маловысотная орбита (100-1000км).



28

Слайд 16. Минимальное угловое расстояние между соседними геостационарными спутниками 3°, поэтому их всего на орбите не более 120.

Геостационарные спутники

Спутник вращаясь на геостационарной орбите, радиус которой – 35 863 км, имеет угловую скорость совпадающую с угловой скоростью вращения Земли, что создаёт иллюзию его неподвижности для наземных антенн.

Достоинства:

- большое количество каналов;
- широковещание и широкий охват территории.

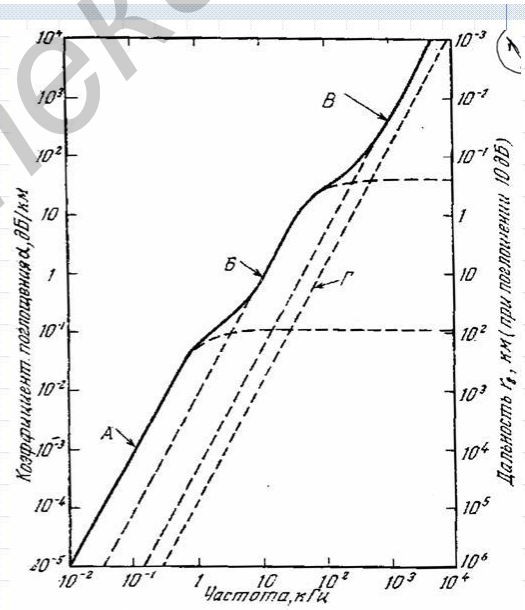
Недостатки:

- значительная удалённость от поверхности Земли;
- принципиальная неустранимость плохой связи для районов близких к Северному и Южному полюсу.

29

Слайд 17. При связи через спутник уже ощущается задержка ≈ 0,2 с из-за конечной скорости света.

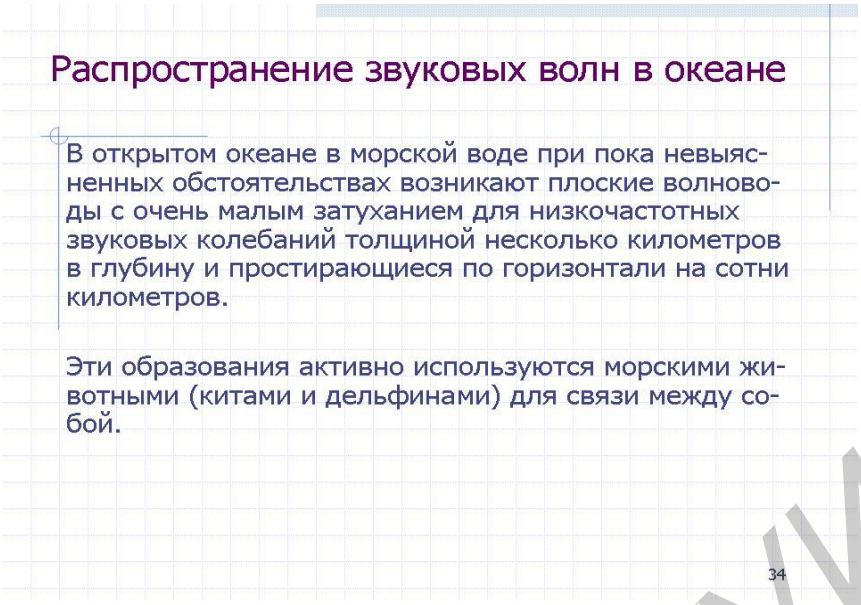
Распространение звуковых волн в океане



Зависимость поглощения в водной среде от частоты звука и расстояния

33

Слайд 18. Сигнал с частотной полосой 1 Гц–1 кГц распространяется в океане на сотни километров с минимальным затуханием.



Слайд 19. Передача информации и связь через гидросферу пока человеком освоена плохо.

В последнее время развивается так называемая звукоподводная связь, осуществляемая в водной среде посредством излучения и приёма модулированных звуковых или ультразвуковых колебаний для двусторонней связи между судами и глубоководными аппаратами, водолазами, аквалангистами. Развитие звукопроводной связи началось с появлением подводных лодок для связи между подводными лодками и надводными кораблями.

Заключение

Для доступа к ресурсам «чужих» компьютеров все компьютеры сети имеют специальный аппаратный модуль, называемый **сетевым адаптером**, который передаёт данные в линию связи совместно с управляющей программой – **драйвером**.

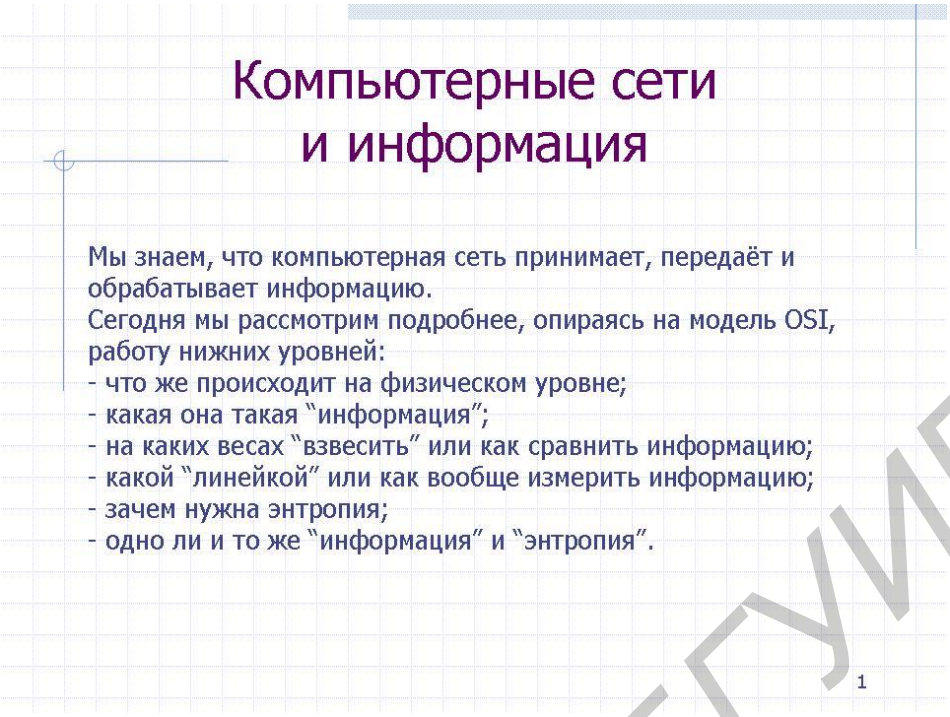
Основными характеристиками передачи трафика через физические каналы являются: скорость передачи данных, ёмкость канала связи, частотная полоса пропускания, погонное затухание в децибелах на единицу длины.

1.3 Лекция. Элементы теории информации

В компьютерных сетях передаются различные данные. Попытаемся понять, что же такое данные и чем они отличаются от информации? Разберём свойства информации, научимся её сравнивать с точки зрения синтаксической, семантической и прагматической адекватности информации. Введём понятие тезаурусной меры.

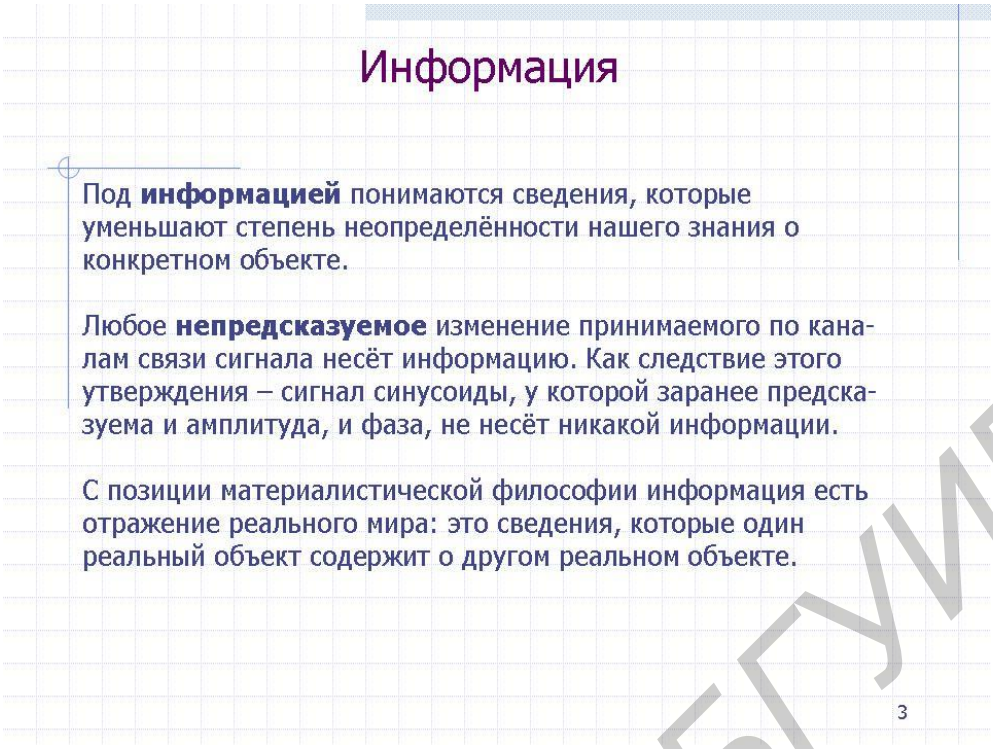
Здесь мы научимся количественно оценивать информацию. А математически формализованное определение информации позволит нам применить ряд полезных соотношений при анализе передачи информации. Мы определим и обсудим единицу информации – **бит**, определяемый как один из альтернативных ответов на двойной вопрос.

В этой лекции для определения информации используется вероятностный подход как наступление некоторого события в результате завершения опыта. Мы определим и разберём родственное информации понятие энтропии и научимся количественно её оценивать.

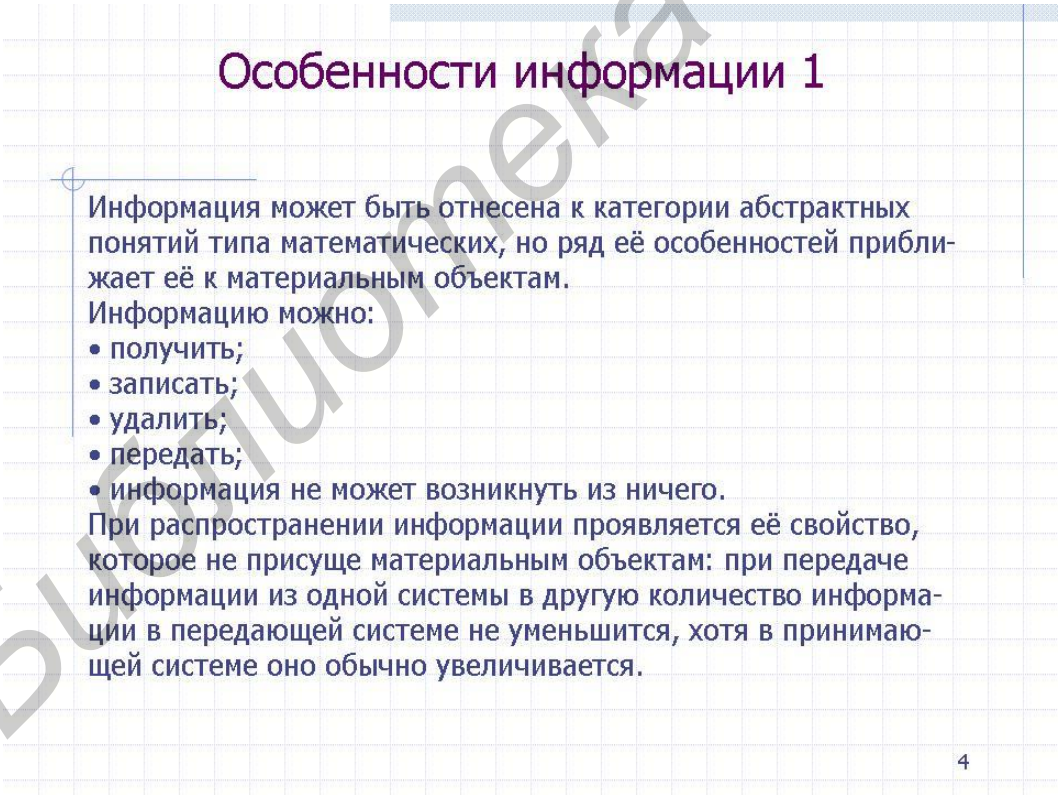


Слайд 1. Основная цель компьютерных сетей – передача и обработка информации.

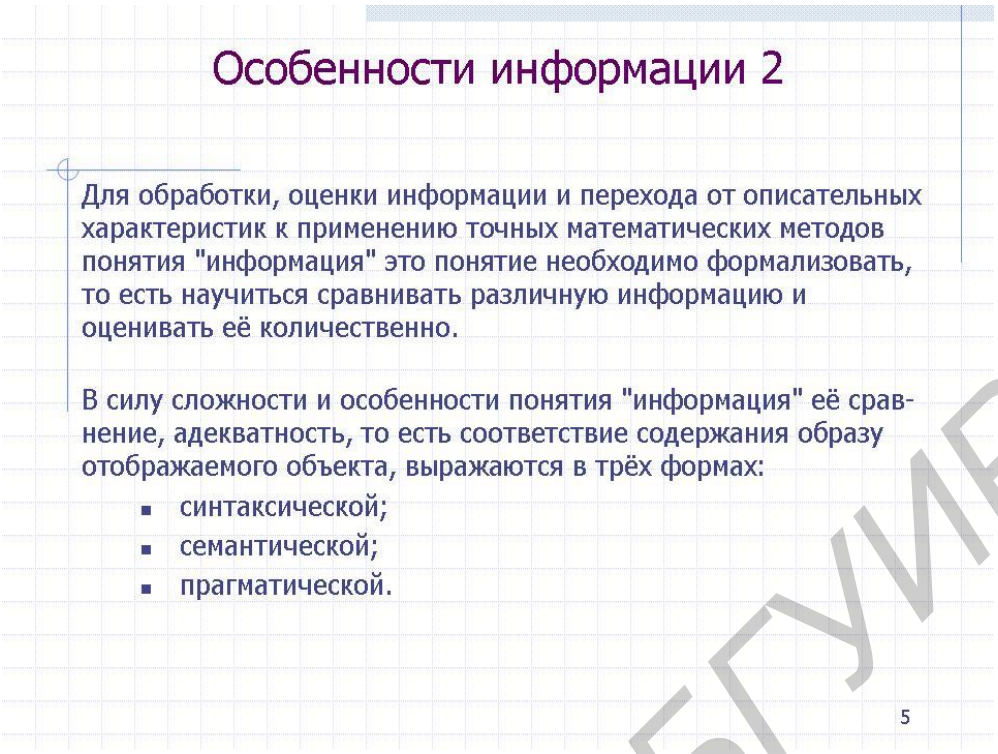
Слайд 2. Анализ передачи информации на уровне битов – это физический уровень.



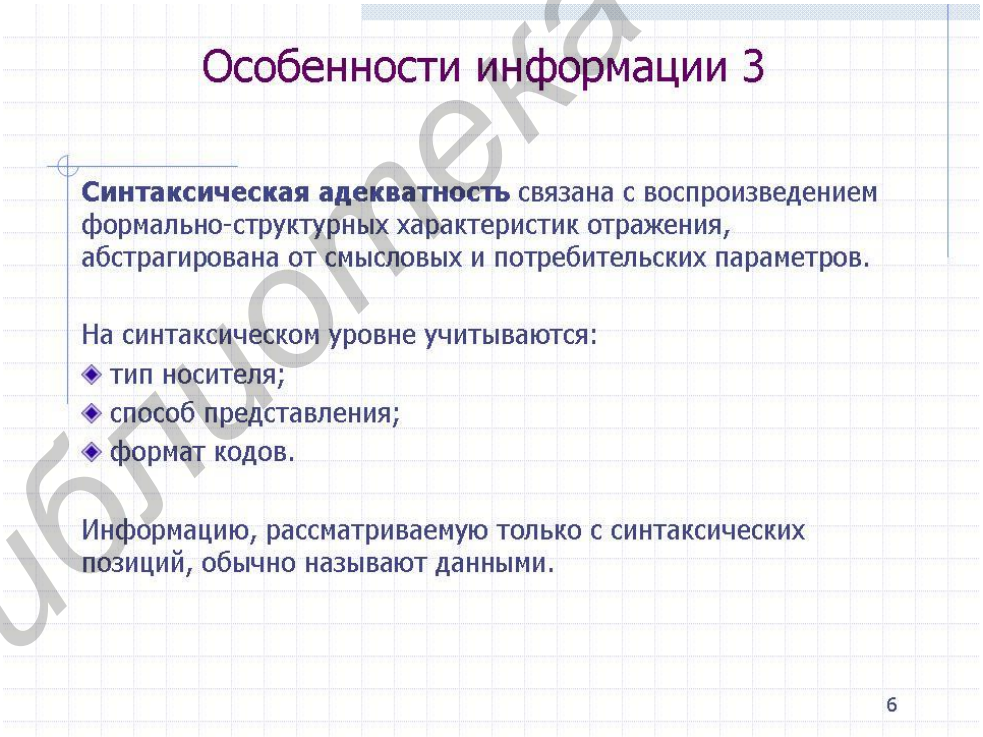
Слайд 3. Информация о неком событии связана с вероятностью возникновения этого события.



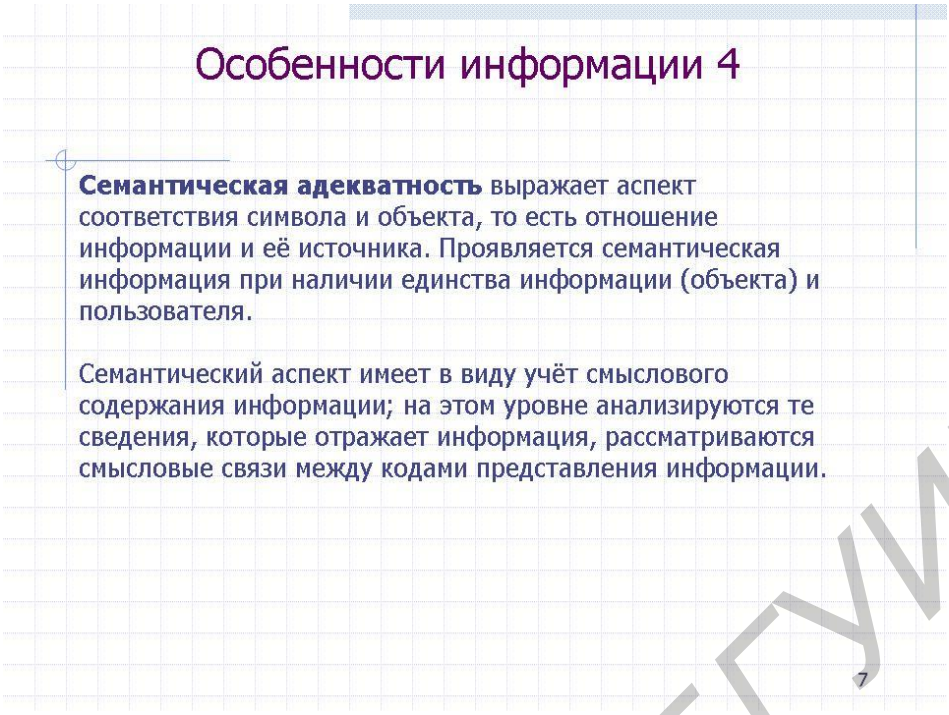
Слайд 4. Информация не материальна, но по свойствам близка к материальным объектам.



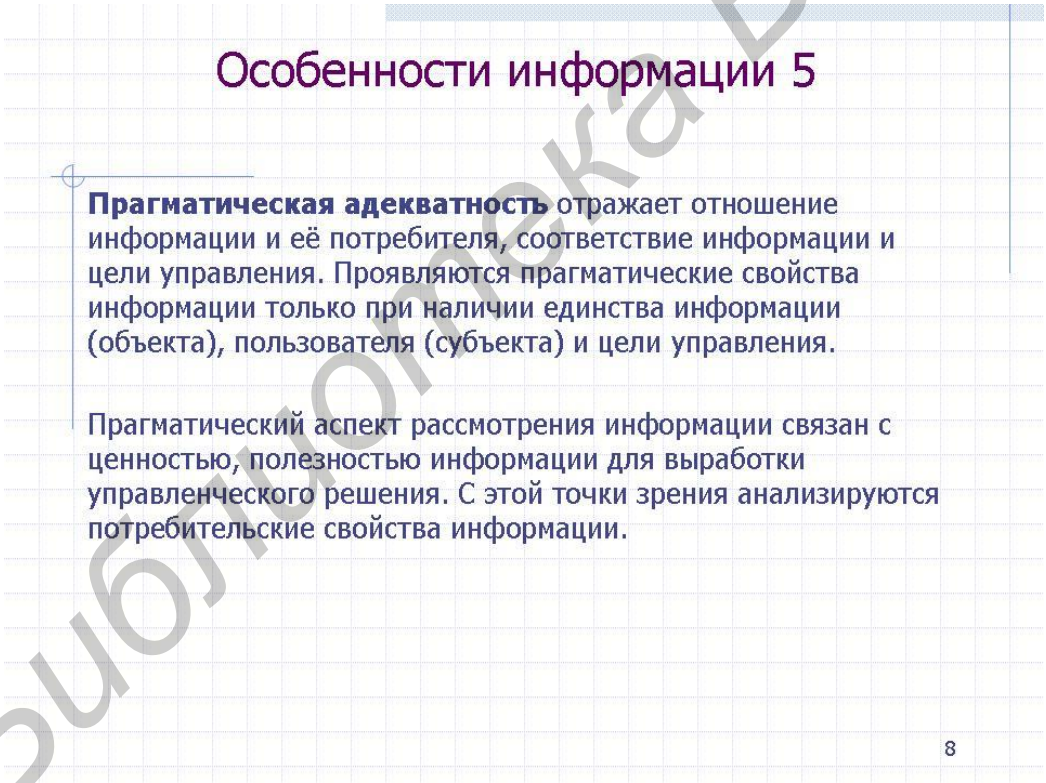
Слайд 5. Для анализа информации необходимо научиться количественно её сравнивать.



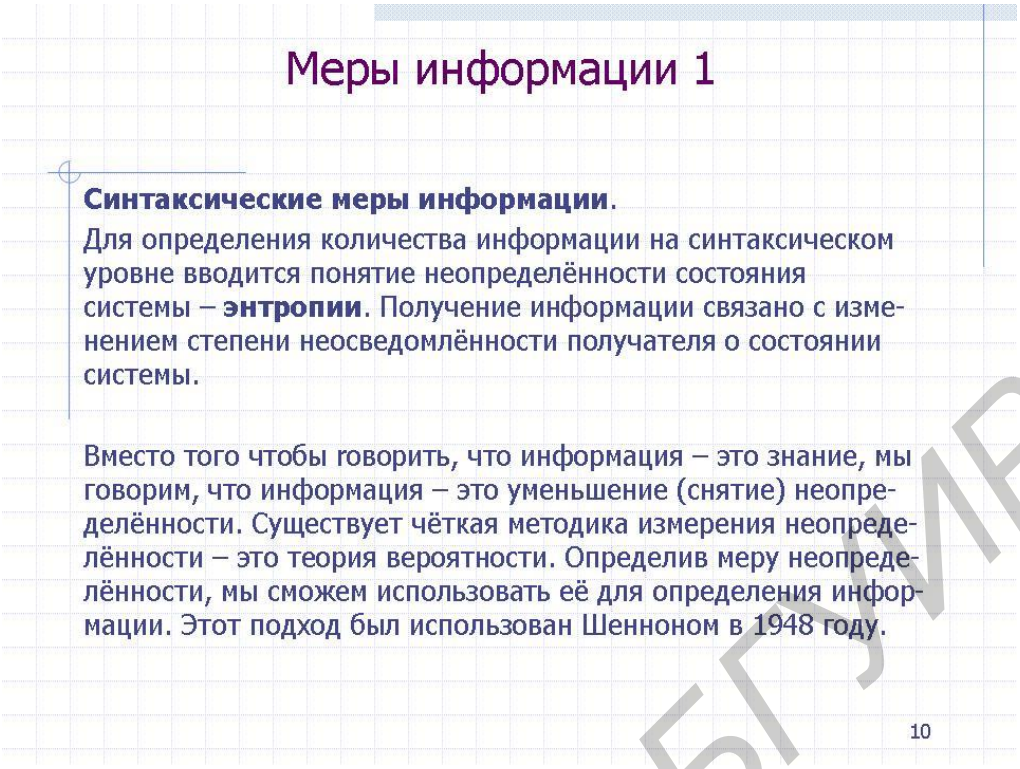
Слайд 6. Синтаксическая форма информации – единственная, которую можно оценить количественно с помощью аппарата теории связи.



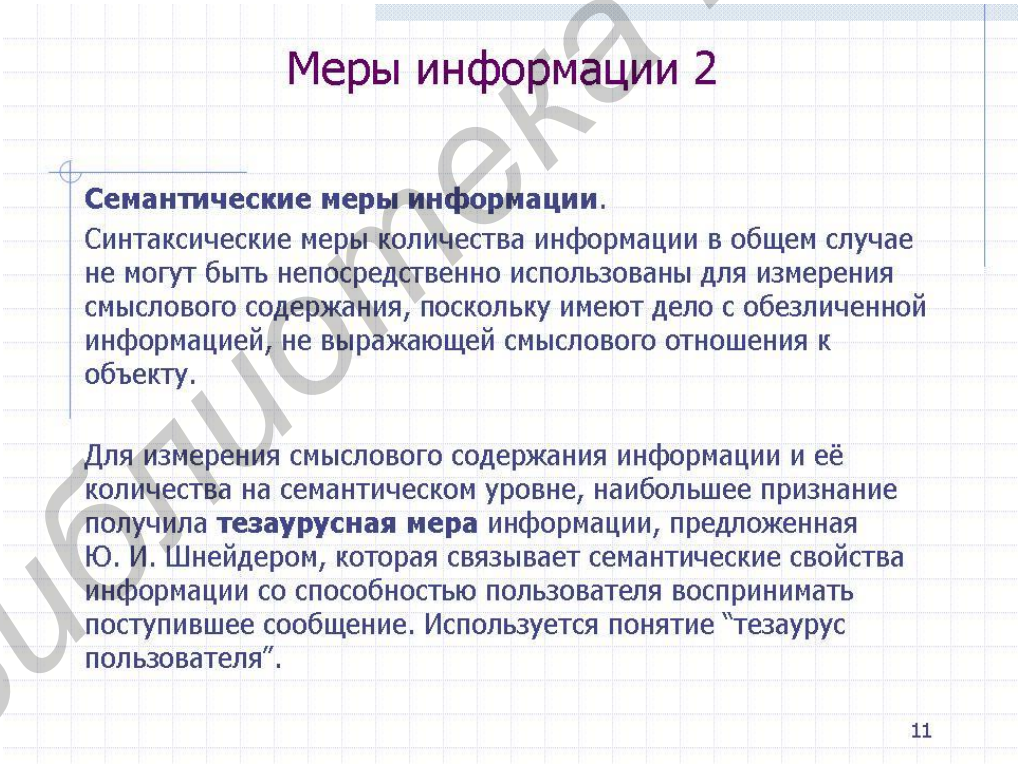
Слайд 7. Семантический или понятийный аспект информации.



Слайд 8. Прагматическая адекватность информации незаменима в экономике и часто соответствует денежному эквиваленту и измеряется в нём.

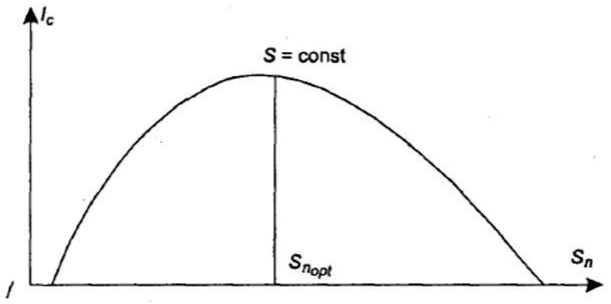


Слайд 9. Одно из основных понятий информации – энтропия.



Слайд 10. Для оценки семантической информации существуют эмпирические методы, основанные на словарях знаний или тезаурусе.

Меры информации 3



Зависимость информации I_c от величины тезауруса S_n

12

Слайд 11. Одна из эмпирических зависимостей для оценки семантической информации.

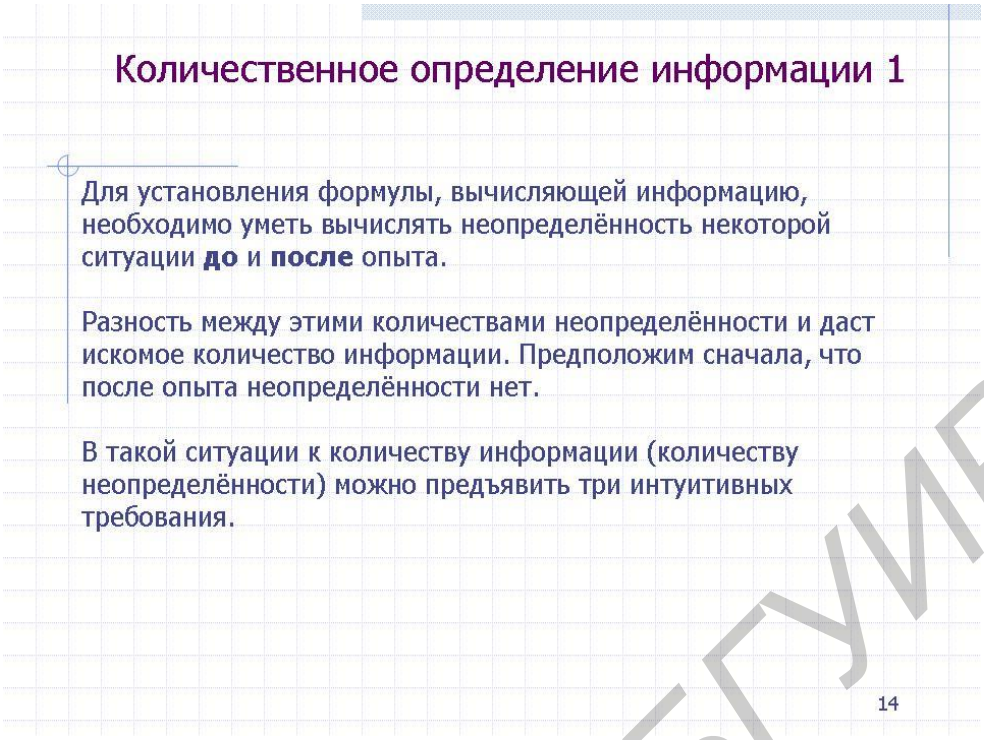
Меры информации 4

Прагматическая мера информации — это полезность информации, её ценность для пользователя (управления). Эта мера также является величиной относительной, обусловленной особенностями использования информации в той или иной системе управления. Ценность информации целесообразно измерять в тех же самых единицах, в которых измеряется целевая функция управления системой.

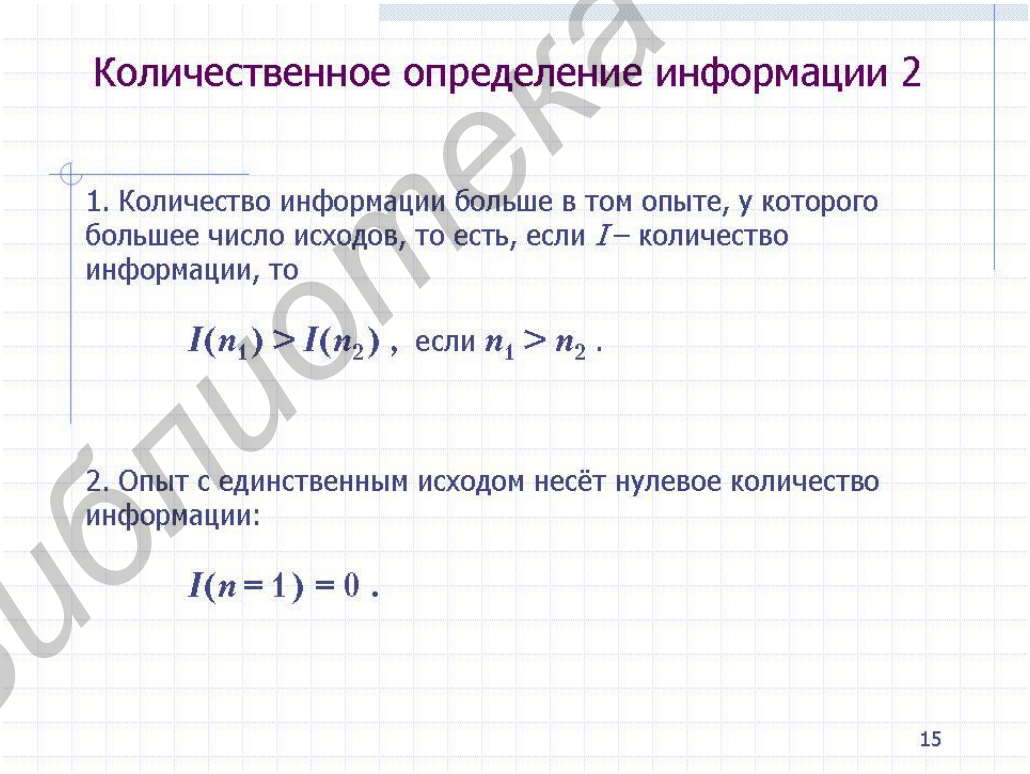
К примеру, в экономических системах самое разумное когда мера информации как-то соотносится с денежным эквивалентом.

13

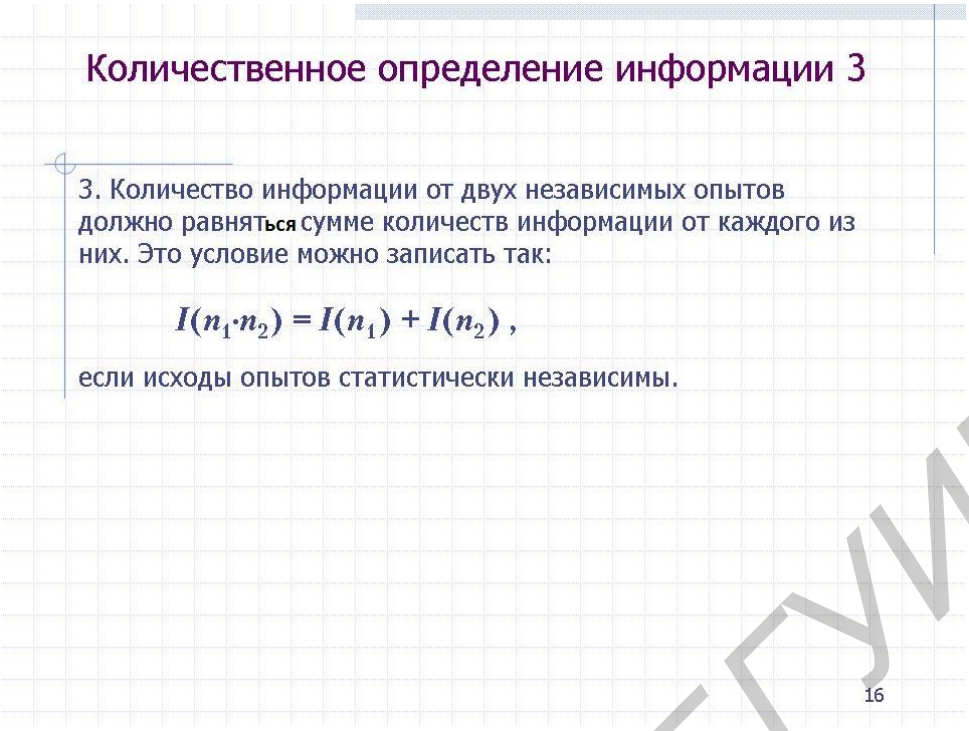
Слайд 12. Прагматическая адекватность не поддаётся математическому формализму и приравнивается, если не к деньгам, то к интуиции.



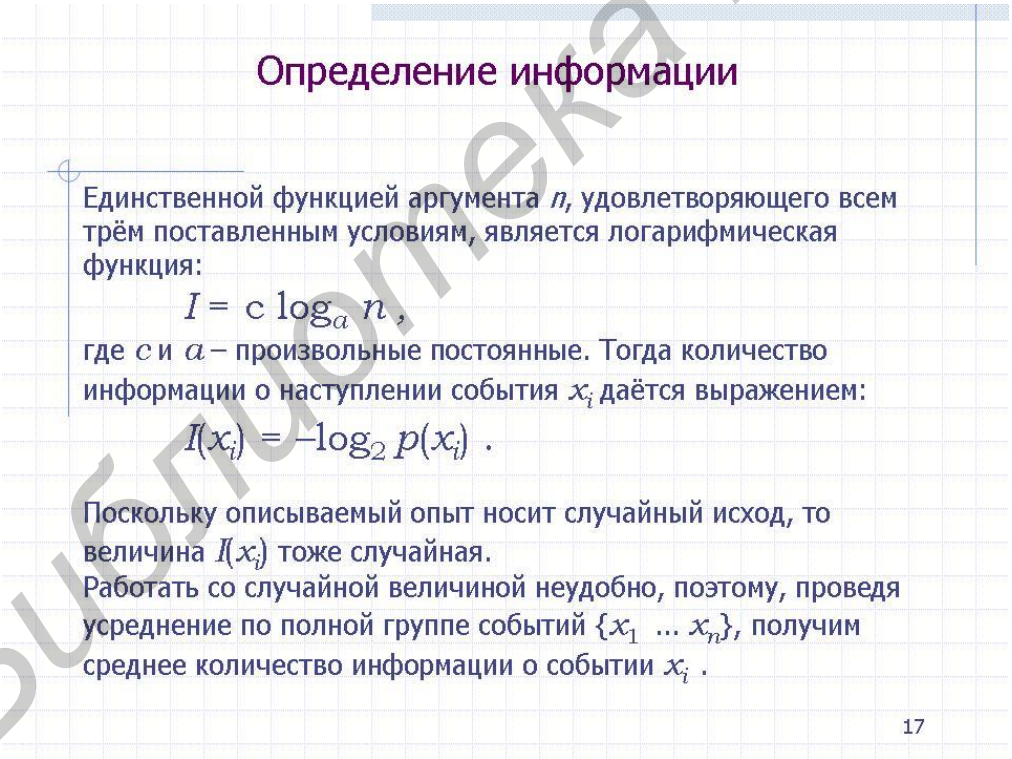
Слайд 13. Нулевая неопределённость после опыта – это нулевая энтропия.



Слайд 14. Количественное определение информации для частного случая, когда неопределённости после опыта нет.



Слайд 15. Количественное определение информации для частного случая, равновероятностного исхода опыта.



Слайд 16. Интуитивное определение информации, предложенное инженером Р. Хартли в 1928 году.

Определение энтропии

$$< I(x_i) >= \sum_{i=1}^{n} I(x_i)p(x_i) = -\sum_{i=1}^{n} p(x_i)\log\, p(x_i)$$

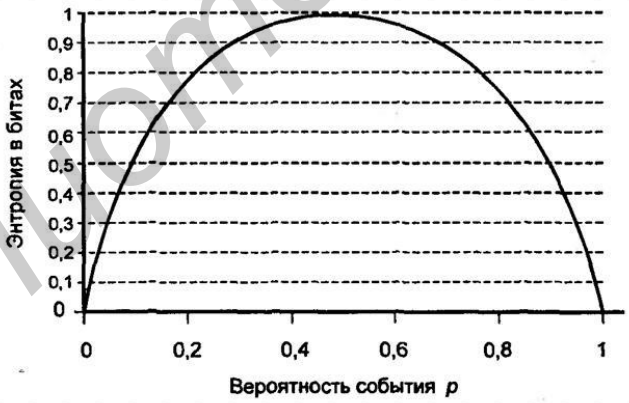
Верхняя формула предполагает отсутствие неопределённости после опыта. Двойственность этого соотношения в том, что если всё-таки **осталась неопределённость после опыта**, то срабатывает нижнее выражение.
Нижнее выражение – это фундаментальное понятие теории информации – **энтропия**, которая выражает среднее количество неопределённости в наступлении того или иного исхода опыта.

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log\, p(x_i)$$

18

Слайд 17. Определение энтропии, предложенное К. Шенноном. Энтропия и информация могут принимать дробные значения.

Количественное определение информации 6



Энтропия двоичной случайной величины для различных вероятностей

19

Слайд 18. Зависимость энтропии опыта с двумя исходами от вероятности событий. Кривая на графике описывает опыт подбрасывания монеты со смещённым центром тяжести.

Взаимная информация 1

Усредняя по всем случайным параметрам получим выражения для общего количества информации о событии X при состоявшемся событии Y:

$$I(Y, X) = H(X) - H(X \mid Y)$$

и

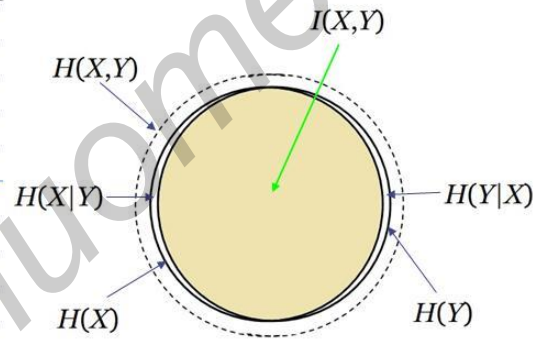
$$I(Y, X) = H(X) + H(Y) - H(X, Y) .$$

Отсюда вытекают свойства количества информации.

34

Слайд 19. Информация о событии ***X*** , содержащаяся в завершившемся опыте ***Y*** [2].

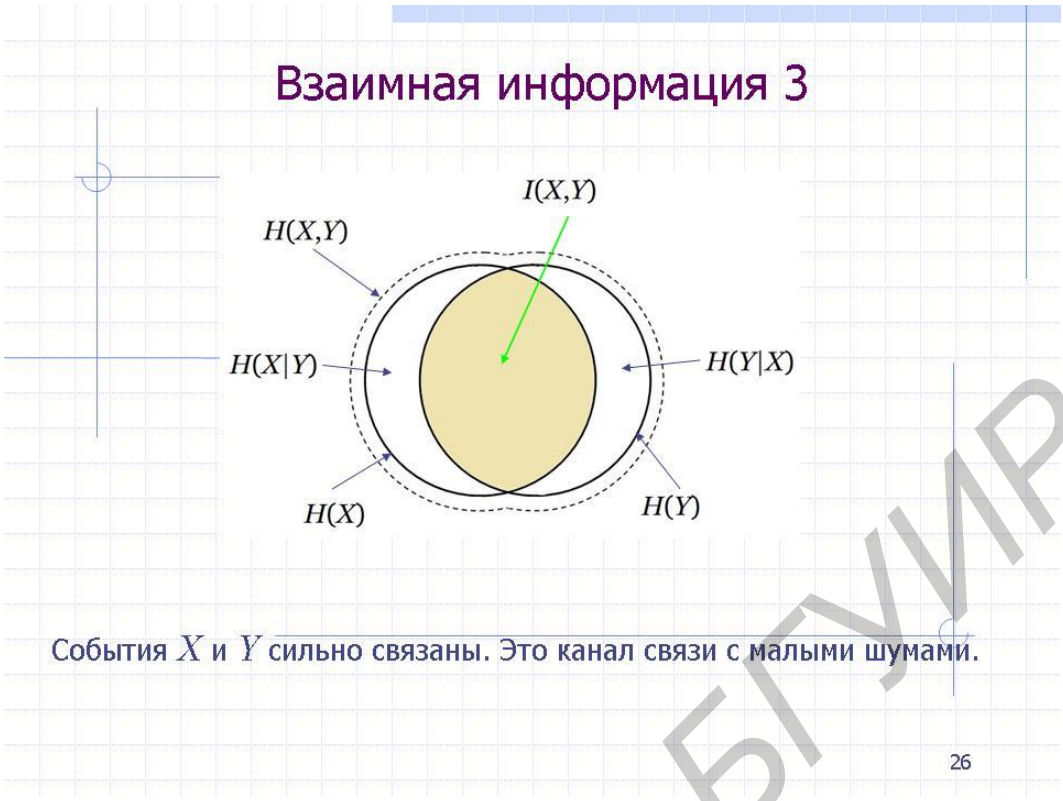
Взаимная информация 2



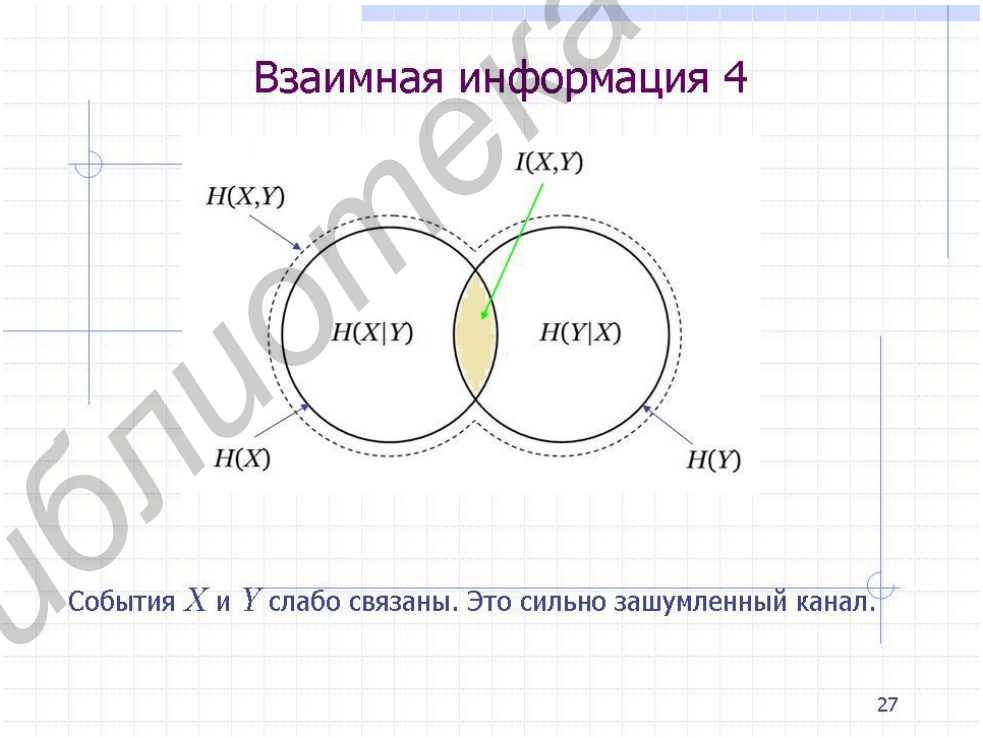
События X и Y почти полностью зависимы. Тогда $I(Y,X) = H(X)$, а условная энтропия $H(X/Y) = 0$. Это канал связи без шумов.

36

Слайд 20. Графическое представление качественной линии связи с очень малыми шумами.



Слайд 21. Графическое представление линии связи с шумами.



Слайд 22. Графическое представление сильно зашумленной линии связи.

Слайд 23. Графическое представление обрыва линии связи. В пунктах, соединённых такой линией связи между событиями ***X*** и ***Y***, нет никакой корреляции – передача информации невозможна.

$$I(X,Y) = 0.$$

Заключение

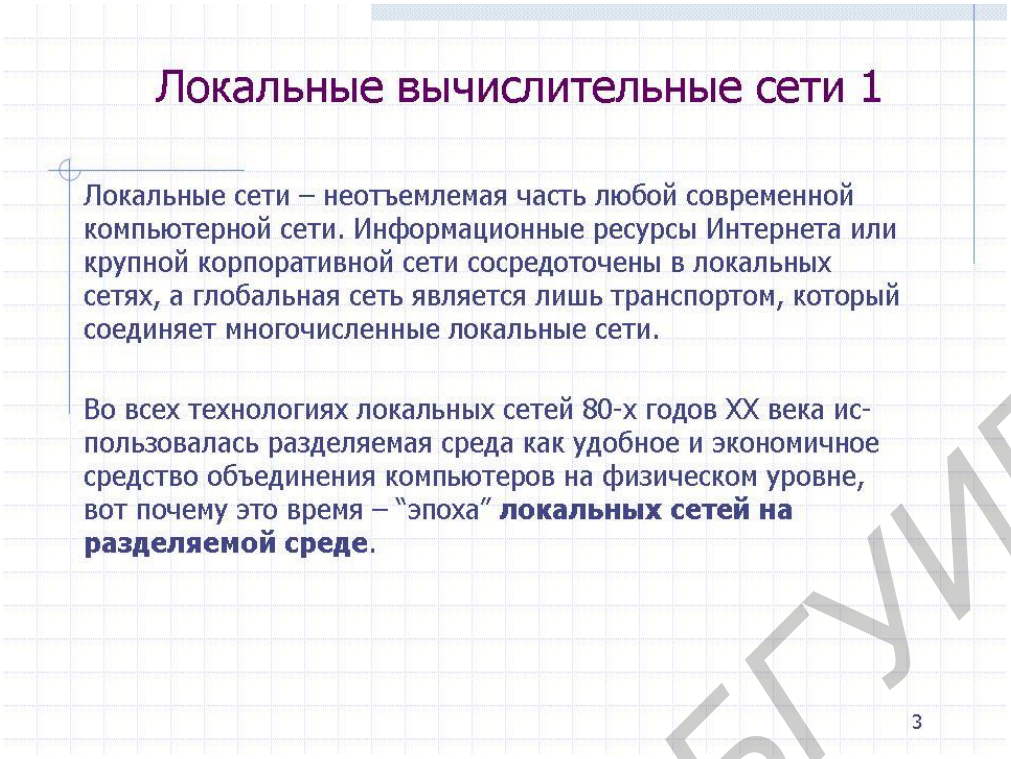
В этой лекции разобраны понятия энтропии и взаимной информации для группы из двух событий. Приведены их основные свойства. Изложенных данных достаточно для понимания дальнейшего материала по компьютерным сетям.

Авторы хотели бы предупредить читателя, что изложенный в этой лекции материал является лишь начальным в теории информации. Авторы не смогли изложить здесь материал по дискретным каналам как с шумами, так и без шумов; здесь также не обсуждаются различные системы кодирования. Эти вопросы требуют громоздкого математического аппарата, большого объёма, времени и излагаются в специальных курсах. Учитывая эти извинительные обстоятельства, авторы хотели бы отослать читателя к замечательной фундаментальной работе [2].

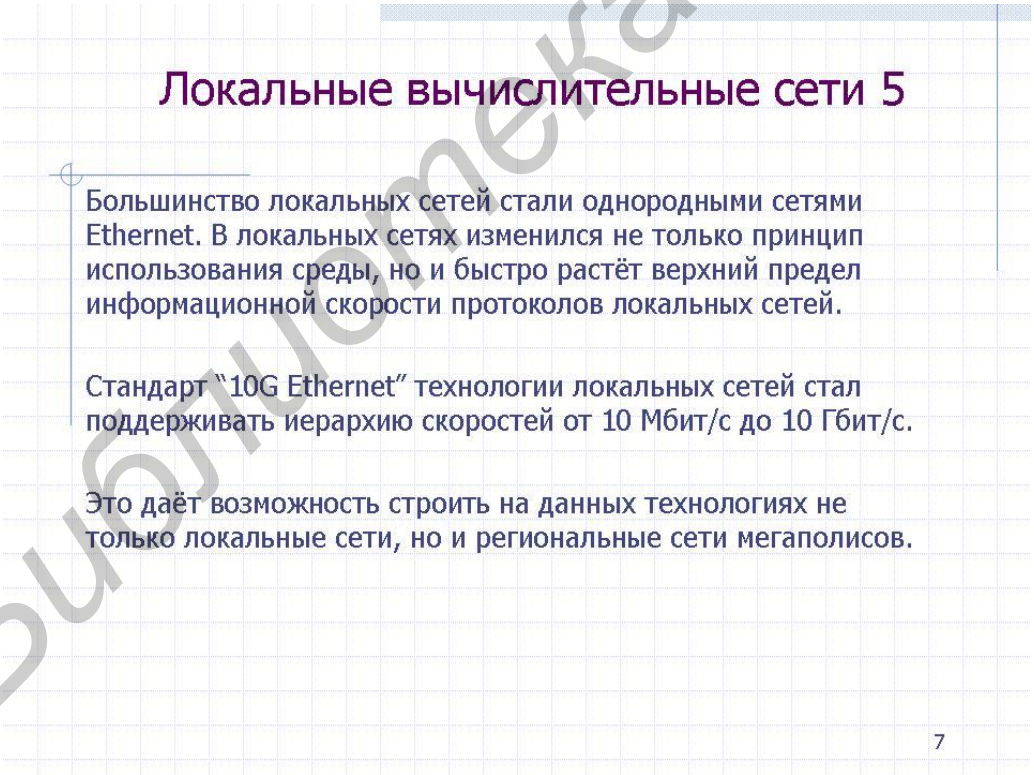
1.4 Лекция. Канальный уровень. Технология Ethernet

Алгоритм доступа к разделяемой среде – главный фактор, определяющий эффективность совместного использования среды. В технологии Ethernet применяется простой алгоритм доступа, позволяющий узлу сети передавать данные в те моменты времени, когда он считает, что разделяемая среда свободна. Простота алгоритма доступа определила простоту и низкую стоимость оборудования Ethernet. Негативным атрибутом алгоритма доступа технологии Ethernet являются коллизии, то есть ситуации, когда кадры, передаваемые разными станциями, сталкиваются друг с другом. Коллизии снижают эффективность разделяемой среды и придают работе сети непредсказуемый характер.

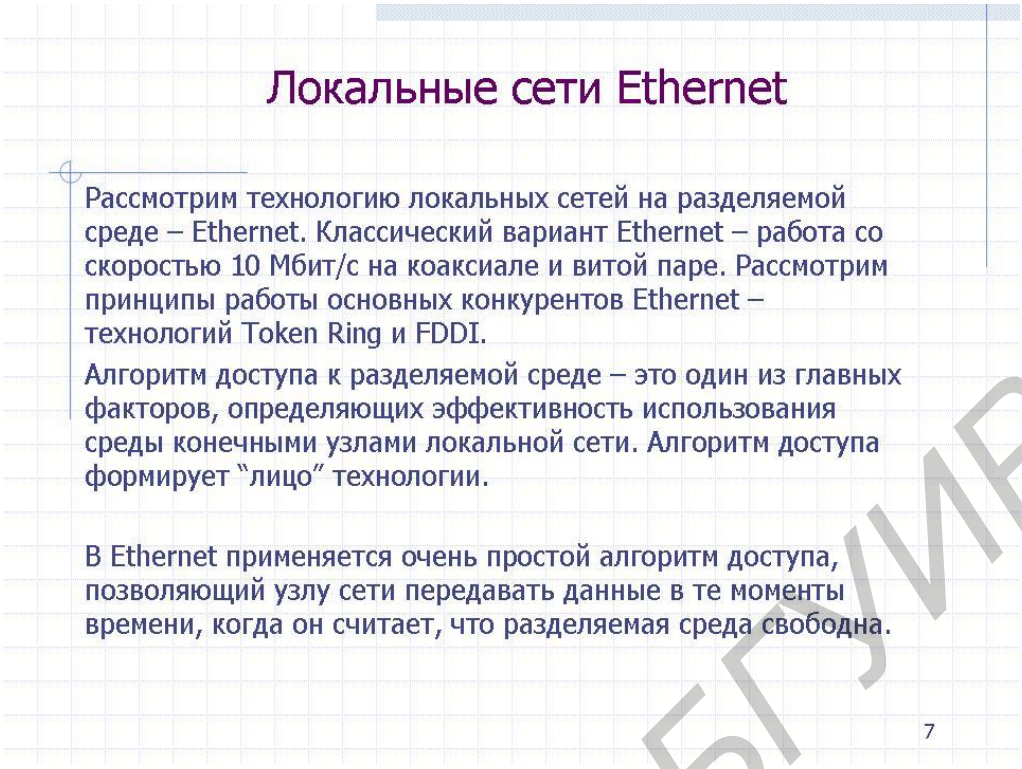
В технологиях Token Ring и FDDI поддерживаются более сложные и эффективные алгоритмы доступа к среде, основанные на передаче друг другу токена – специального маркера, разрешающего доступ.



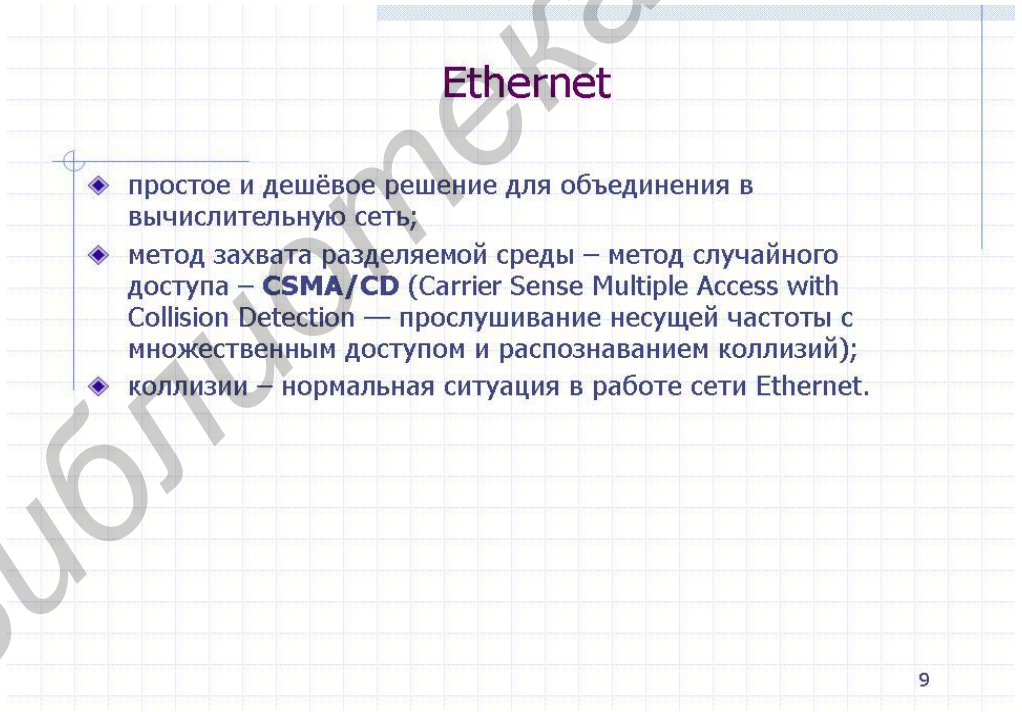
Слайд 1. Передача данных в локальных сетях происходит на канальном уровне модели OSI.



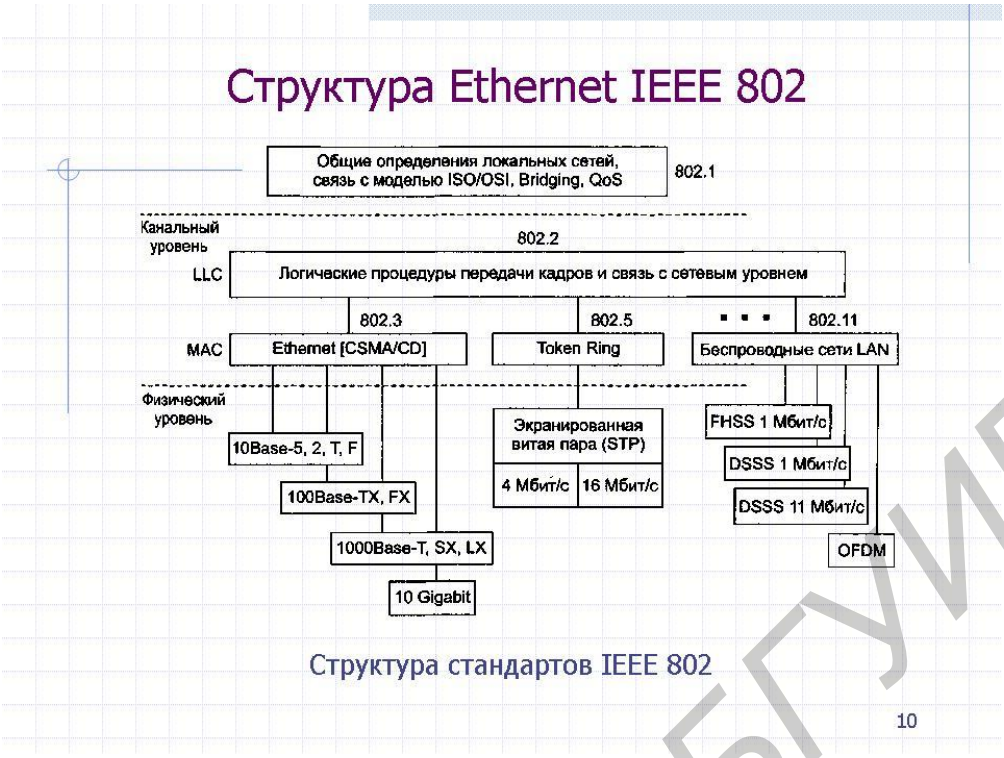
Слайд 2. Сети Ethernet могут работать и на витой паре, и на коаксиальном кабеле, и на оптоволоконном кабеле.



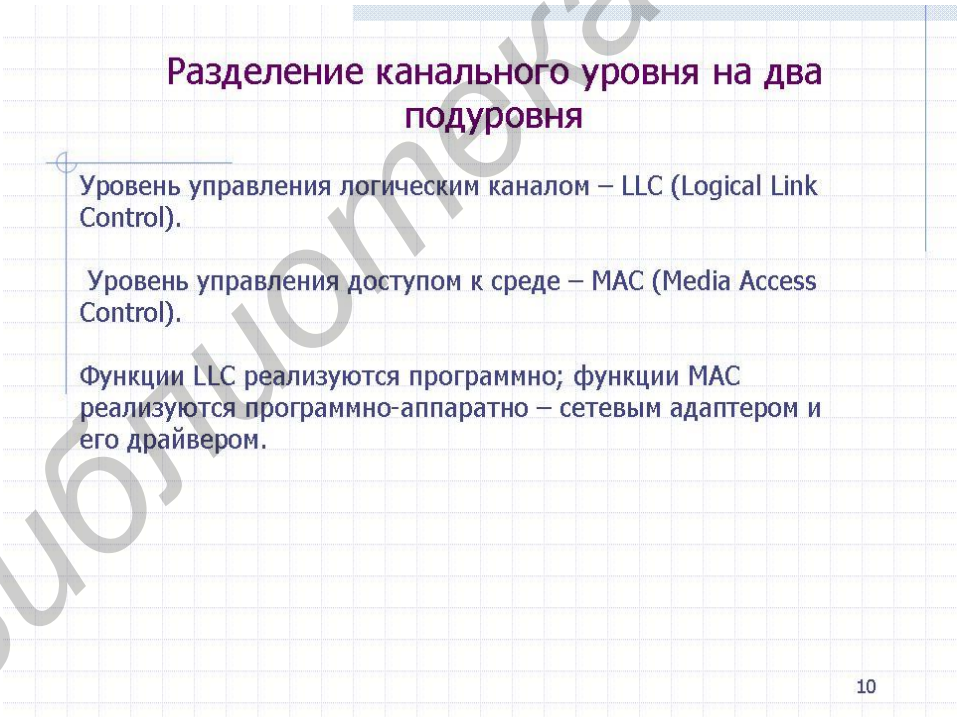
Слайд 3. Ethernet, Token Ring и FDDI – технологии, работающие на канальном уровне в локальных компьютерных сетях.



Слайд 4. Одни из причин победы метода Ethernet – приемлемость конфликта в сети и простота алгоритма разрешения такой коллизии.



Слайд 5. Ethernet в настоящее время достаточно хорошо описан стандартами и нормативными регламентными документами.

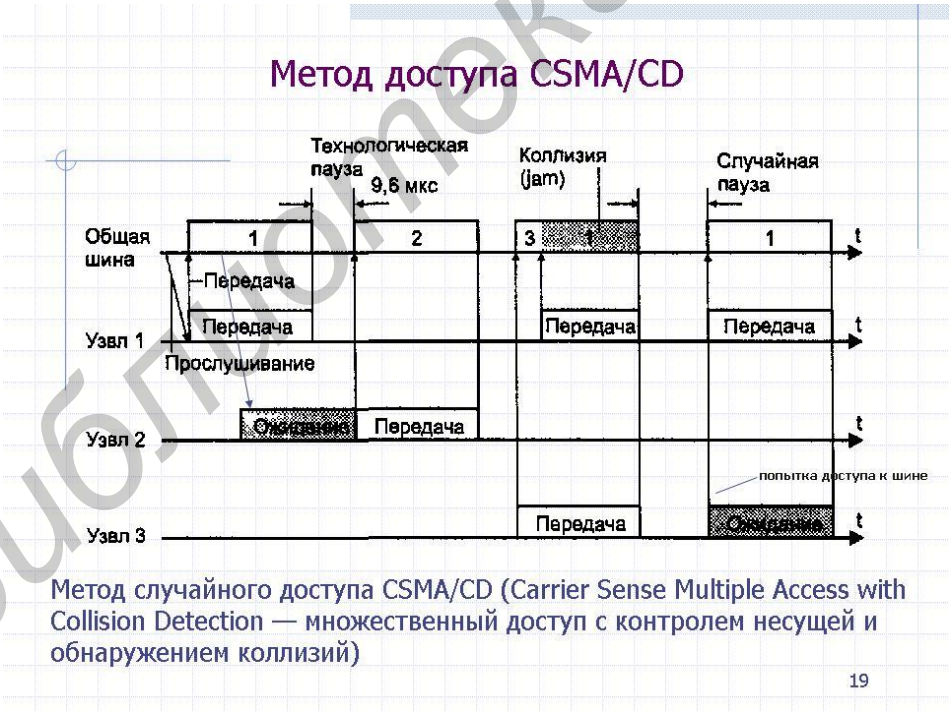


Слайд 6. Канальный уровень очень сложен. Для безотказной работы он разбит на **логический** подуровень и подуровень **доступа к среде**.

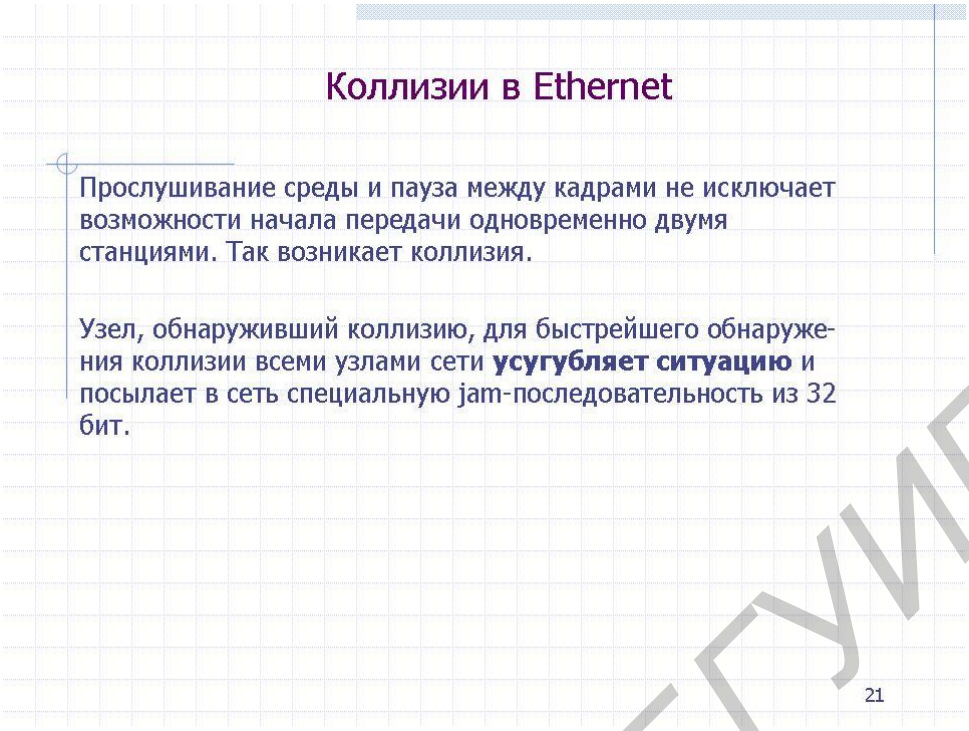
Слайд 7. Вторая причина победы Ethernet – совершенно простая структура кадра, в который упакованы передаваемые по сети данные.

Слайд 8. В сетях с коммутацией пакетов данные дробятся на доли. Эти доли на каждом уровне имеют свои названия.

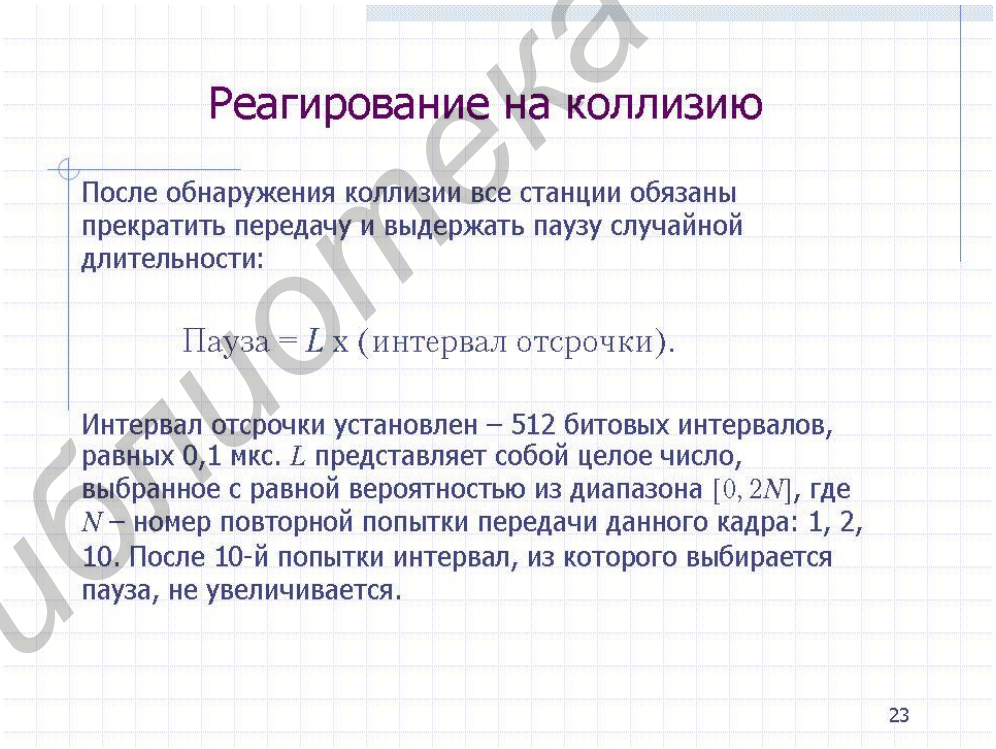
Слайд 9. Названия протокольных долей данных ни в коем случае не являются синонимами, рисунок иллюстрирует это.



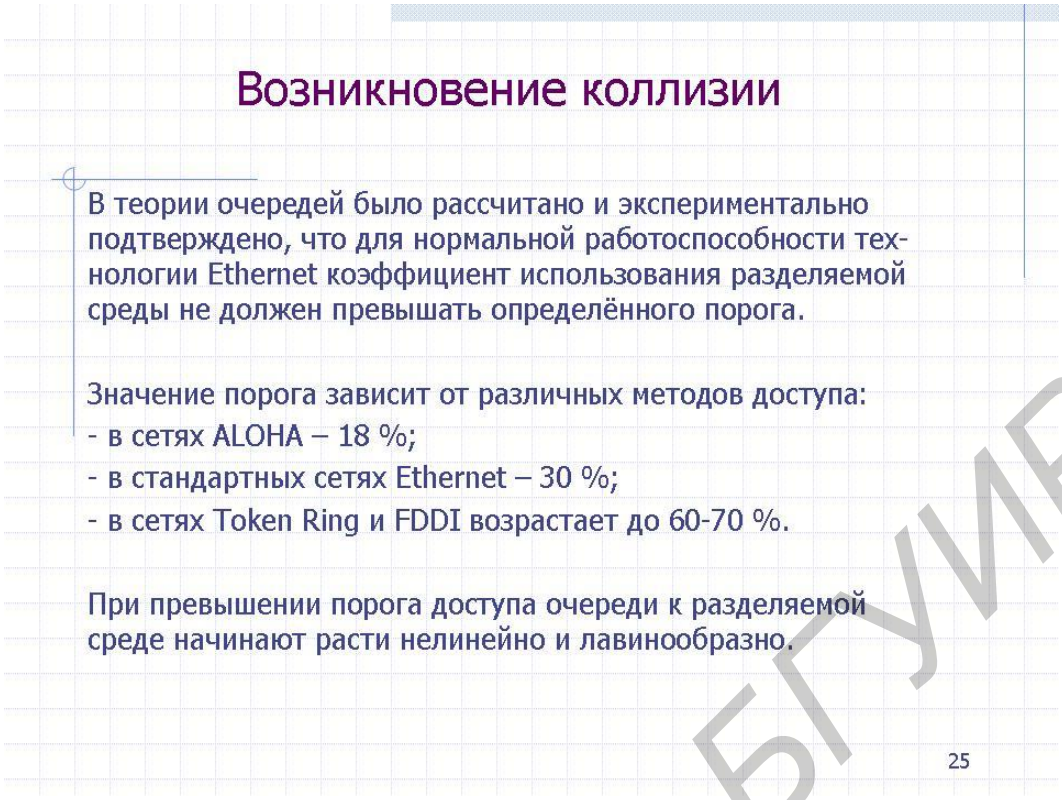
Слайд 10. Временна́я диаграмма возникновения конфликта в локальной сети Ethernet.



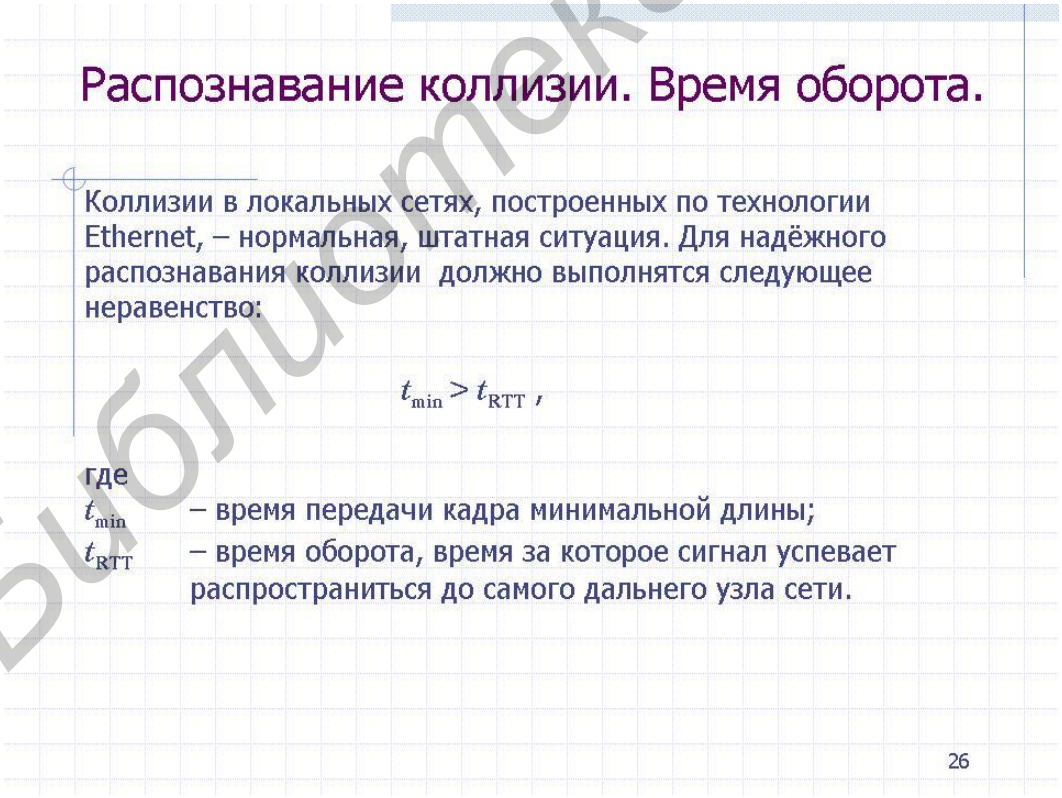
Слайд 11. Чем быстрее конфликт обнаружен и ликвидирован, тем скорее можно вернуться к нормальной работе.



Слайд 12. После конфликта каждая станция в сети перед возобновлением работы должна выдержать статистически случайную паузу.



Слайд 13. Расплата за простоту Ethernet произошла дорогой ценой – использование разделяемой среды не может превысить 30 %.



Слайд 14. Условие для надёжного распознавания конфликта.

Распознавание коллизии

Требование $t_{min} > t_{RTT}$ имеет одно интересное следствие: чем выше скорость протокола, тем меньше должна быть максимальная длина сети.

Для Ethernet на разделяемой среде:

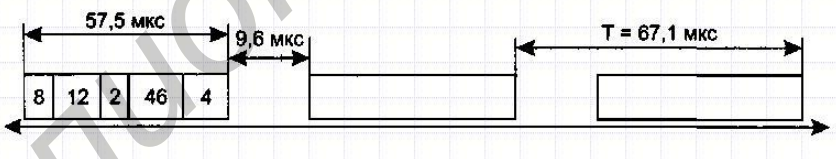
скорость 10 Мбит/с — длина сети до 2500 м;
скорость 100 Мбит/с — длина сети до 250 м;
скорость 1000 Мбит/с — до 25 м.

Эта зависимость, наряду с резким ростом задержек при повышении загрузки сети, свидетельствует о коренном недостатке метода доступа CSMA/CD.

28

Слайд 15. Ещё одна расплата за простоту Ethernet: длина максимального сегмента локальной сети уменьшается при увеличении номинальной скорости протокола.

Ethernet – максимальная производительность 1

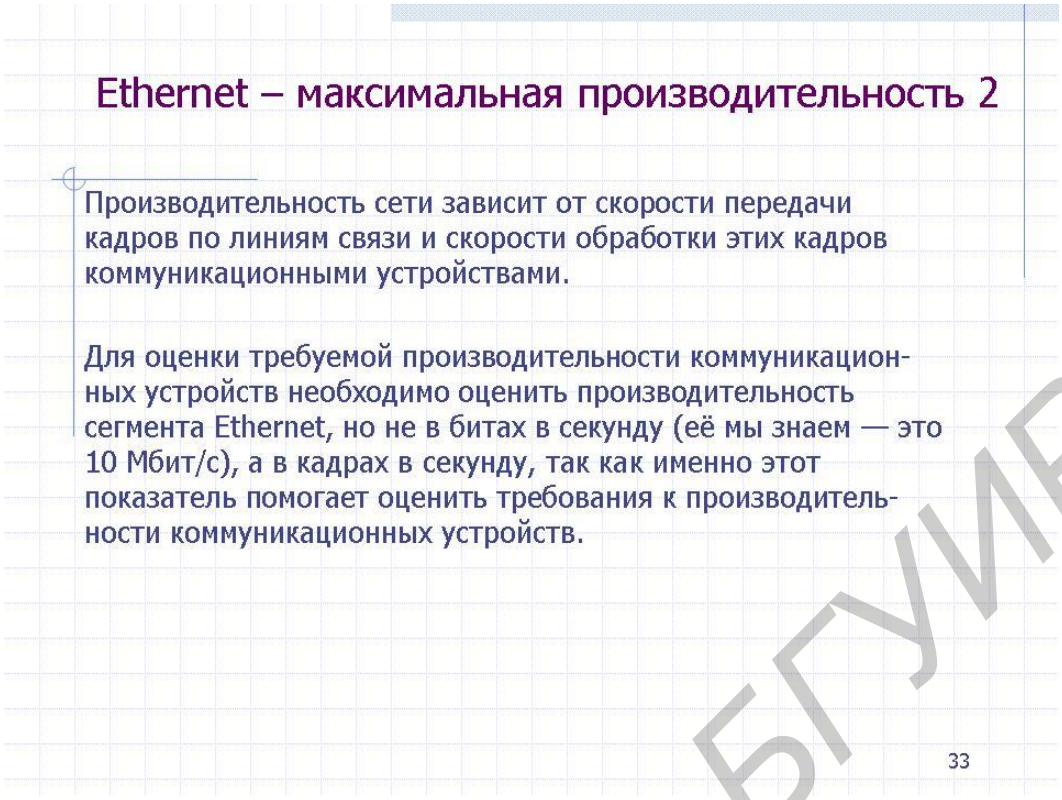


Расчёт пропускной способности Ethernet

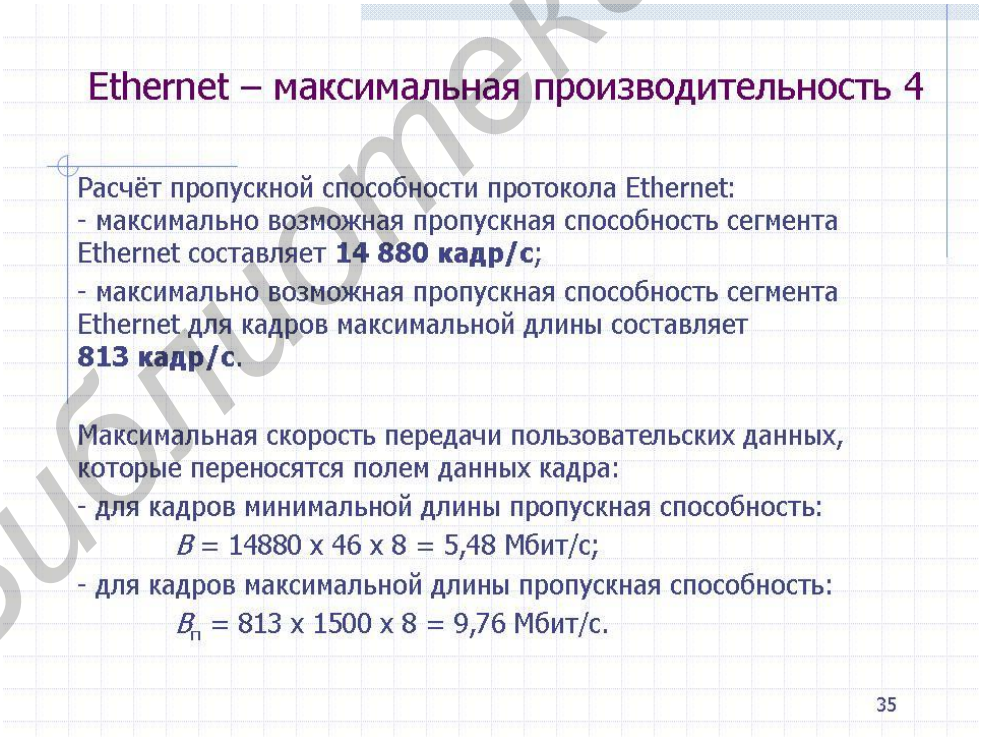
Скорость, с которой протокол передаёт биты по линии связи, называется номинальной скоростью протокола.

32

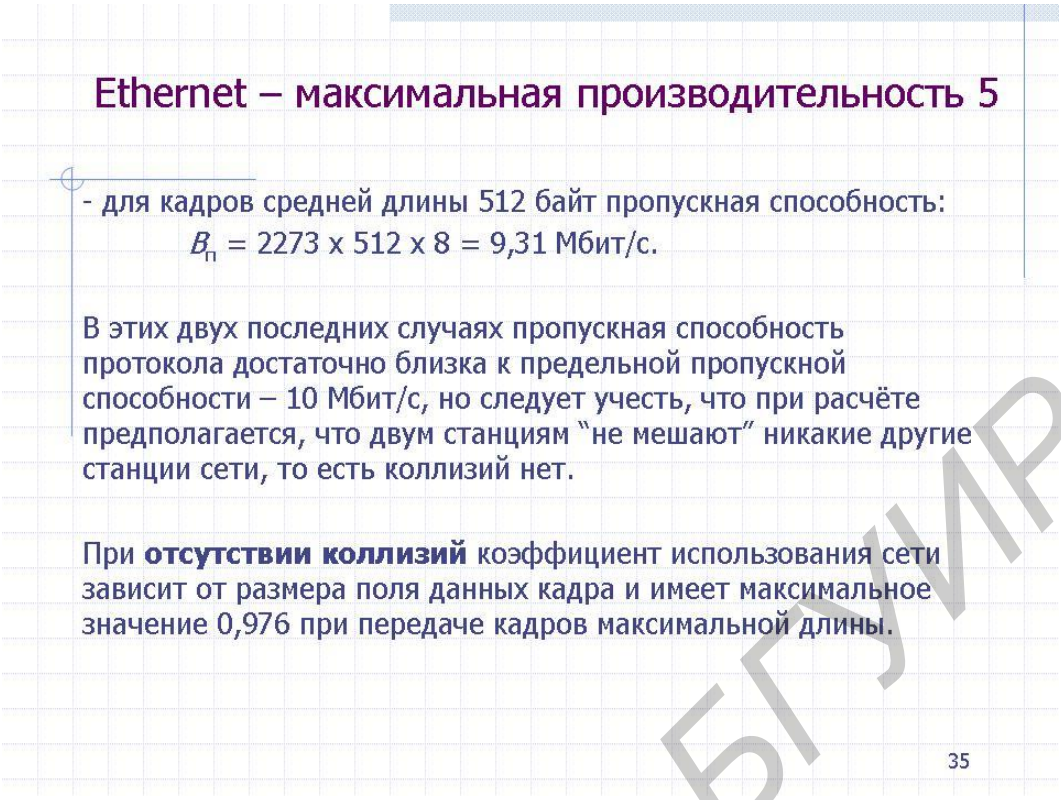
Слайд 16. Какова покадровая производительность Ethernet?



Слайд 17. Следует ожидать, что больших кадров в единицу времени будет передано по сети меньше, чем маленького размера.



Слайд 18. Максимальная скорость передачи пользовательских данных близка к номинальной скорости протокола.



Слайд 19. Не следует забывать, что максимальная скорость передачи пользовательских данных приближается к номинальной скорости протокола лишь в нереальном, теоретическом случае отсутствия коллизий. Наверное, такое возможно, если в локальной сети Ethernet работают всего две станции. Но как только в сети появятся дополнительные станции, – появятся коллизии и скорость передачи данных упадёт.

Заключение

Локальные сети на разделяемой среде – это наиболее простой и дешёвый в реализации тип локальных сетей. Основной недостаток разделяемых локальных сетей состоит в плохой масштабируемости, так как при увеличении числа узлов сети снижается доля пропускной способности, приходящаяся на каждый узел.

При сильной нагрузке сети Ethernet, когда коэффициент использования среды растёт, значительно возрастает время ожидания, поэтому максимальный коэффициент использования среды не должен превышать 30 %.

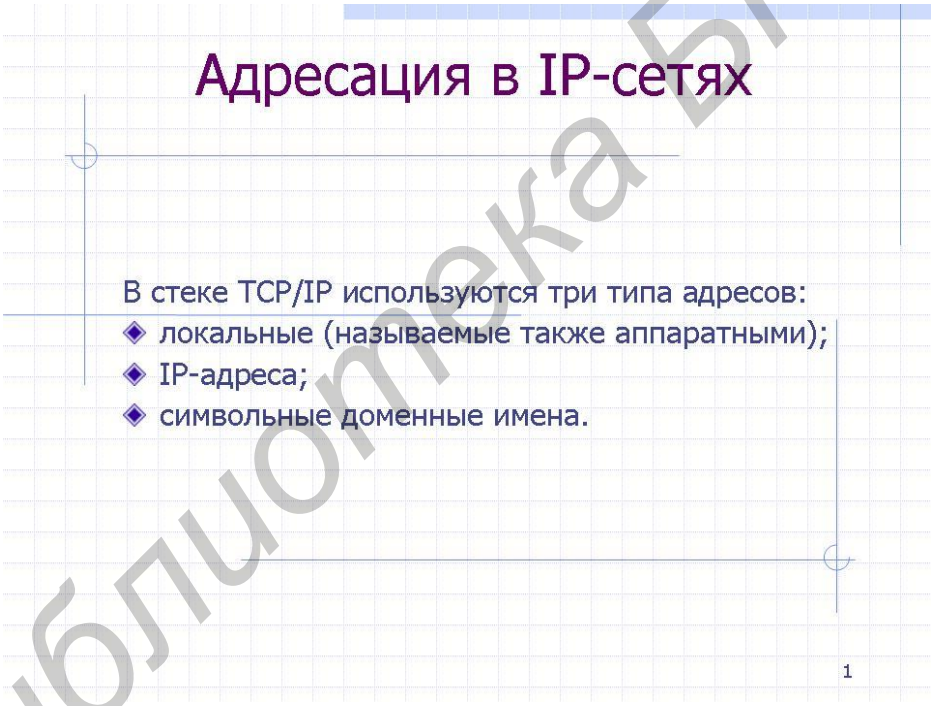
Эта дорогая плата – недогруженности трафика сети на 70 % – следствие дешевизны и простоты метода Ethernet.

1.5 Лекция. Адресация в IP-сетях

Адресация в технологии TCP/IP решает следующие задачи:

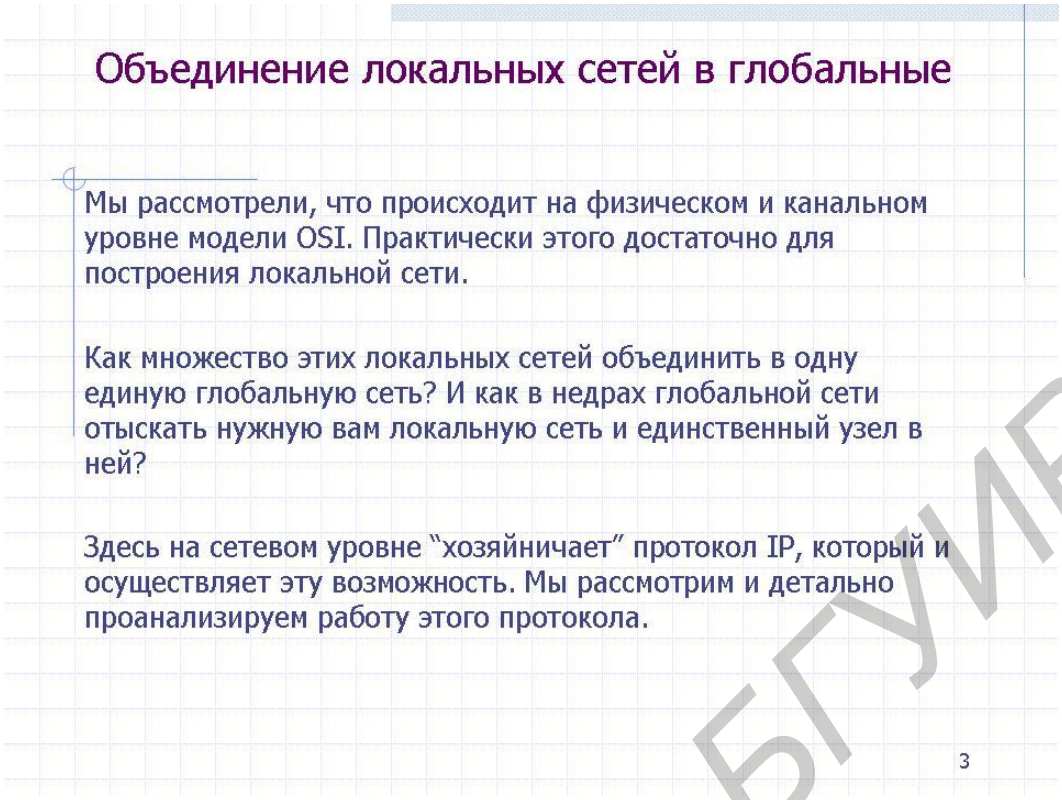
- согласованное использование адресов различного типа: преобразование сетевого IP-адреса в локальный, доменного имени – в IP-адрес;
- обеспечение уникальности адресов подразумевает однозначность адресации в пределах компьютера, подсети, корпоративной сети или Интернета;
- конфигурирование сетевых интерфейсов и сетевых приложений.

Каждая из перечисленных задач имеет простое решение для сети, число узлов которой не превосходит нескольких десятков. Однако в крупных сетях эти же задачи усложняются и требуют принципиально других решений.

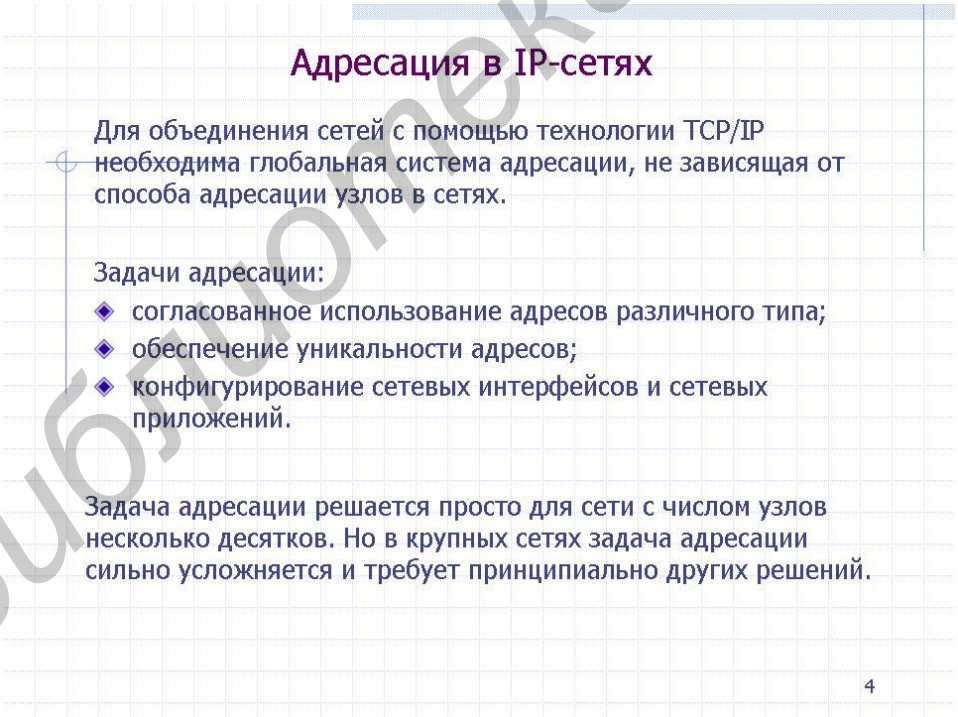


Слайд 1. Глобальные сети используют три типа адресов.

Слайд 2. IP-адресация необходима в глобальных сетях и используется на сетевом уровне. MAC-адреса – основа передачи данных в локальных сетях на канальном уровне.



Слайд 3. Глобальная сеть и Интернет – это следующий уровень иерархии сетей, это объединение локальных сетей.



Слайд 4. IP-адресация в отличие от MAC-адресов создаёт уникальность ресурсов глобальной сети и Интернета.

Схема стека протоколов TCP/IP

Прикладной уровень соответствует трём верхним уровням модели OSI.

Существенным отличием архитектуры стека TCP/IP от многоуровневой архитектуры других стеков является интерпретация функций самого нижнего уровня — уровня сетевых интерфейсов: лишь только организовать взаимодействие с подсетями разных технологий.

Прикладной уровень	FTP, Telnet, HTTP, SMTP, SNMP, TFTP
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, ICMP, RIP, OSPF
Уровень сетевых интерфейсов	Не регламентируется

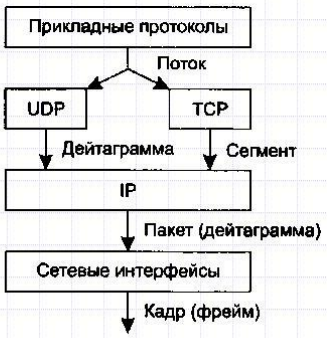
Структура стека TCP/IP

5

Слайд 5. Упрощения стека протоколов TCP/IP по сравнению с моделью OSI, способствовавшие широкому распространению этого стека протоколов при построении компьютерных сетей.

Схема стека протоколов TCP/IP

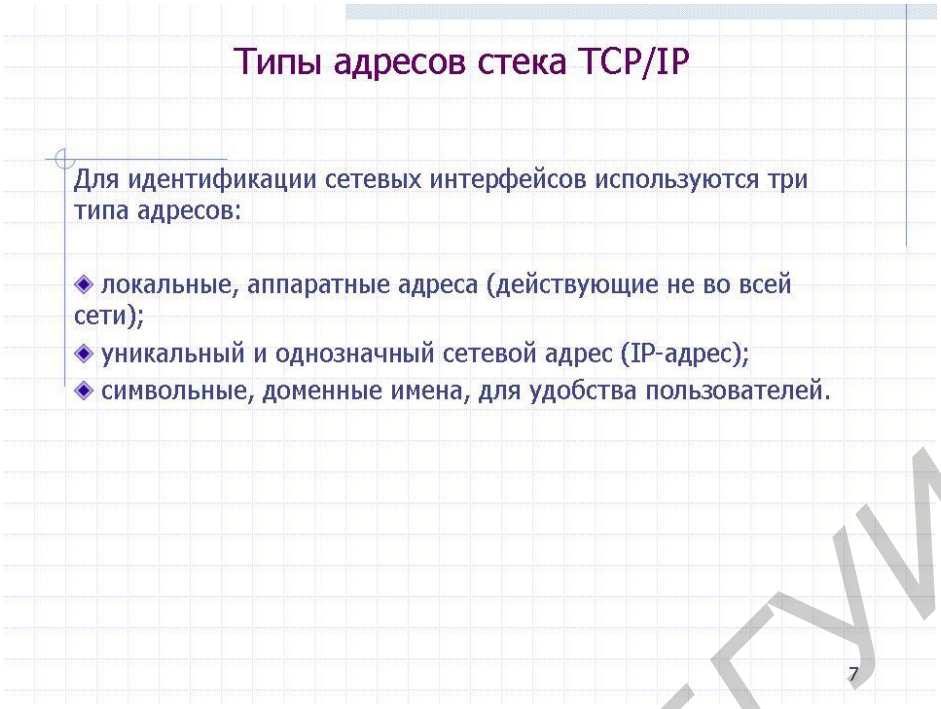
Каждый коммуникационный протокол оперирует некоторой единицей передаваемых данных. Названия этих единиц иногда закрепляются стандартом, а чаще просто определяются традицией.



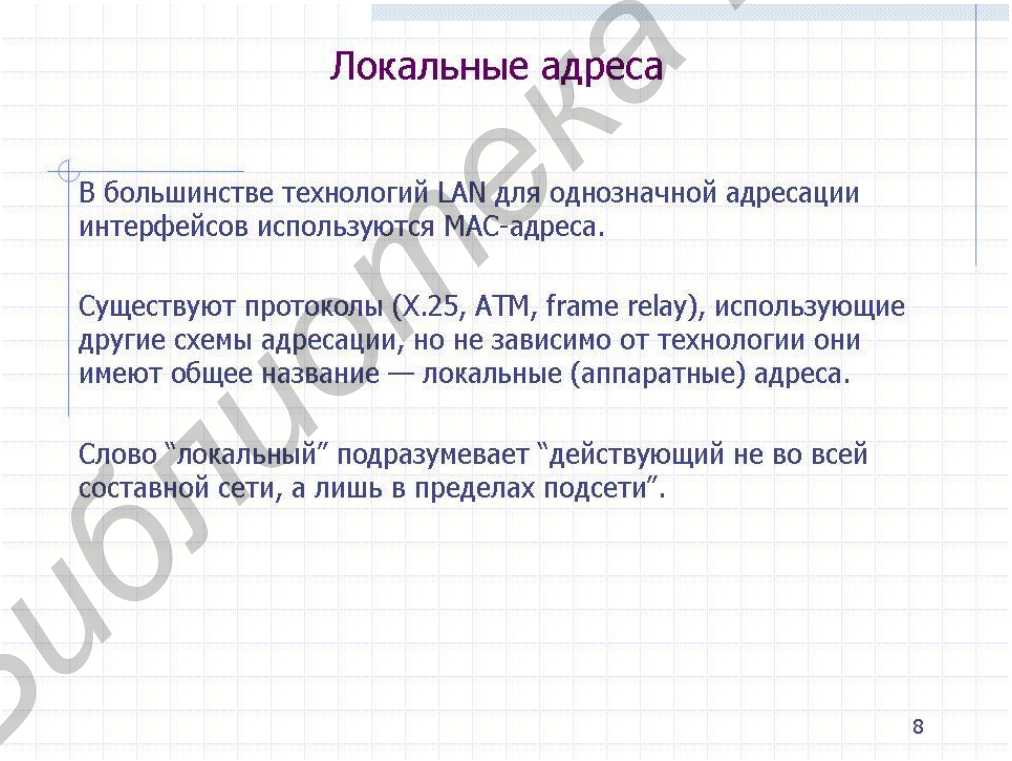
Протокольные названия единиц данных в TCP/IP

6

Слайд 6. Схема взаимодействия протоколов при инкапсуляции пакетов.



Слайд 7. В глобальной компьютерной сети для адресации ресурсов используется несколько типов адресов.



Слайд 8. Некоторые типы адресов используются только для локальных сетей.

Сетевые IP-адреса

Для объединения сетей с помощью технологии TCP/IP необходима глобальная система адресации, не зависящая от способа адресации узлов в сетях.

Решением является уникальная нумерация всех сетей составной сети, а затем нумерация всех узлов в пределах каждой из этих сетей.

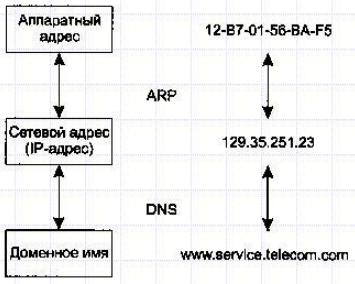
9

Слайд 9. Локальные сети объединяются в глобальные с помощью IP-адресов.

Типы адресов стека TCP/IP

В IP-сетях маршрутизатор может обслуживать сразу несколько сетей, тогда каждый его интерфейс имеет собственный IP-адрес.

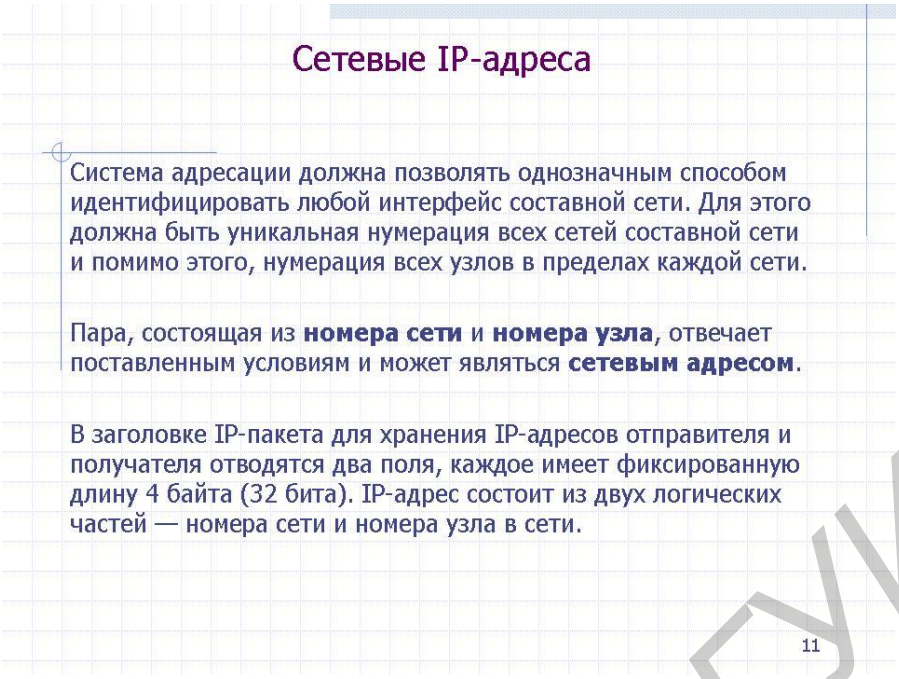
Все сети и узлы в них имеют уникальный составной номер: номер сети и номер узла. Такой адрес называется IP-адресом.



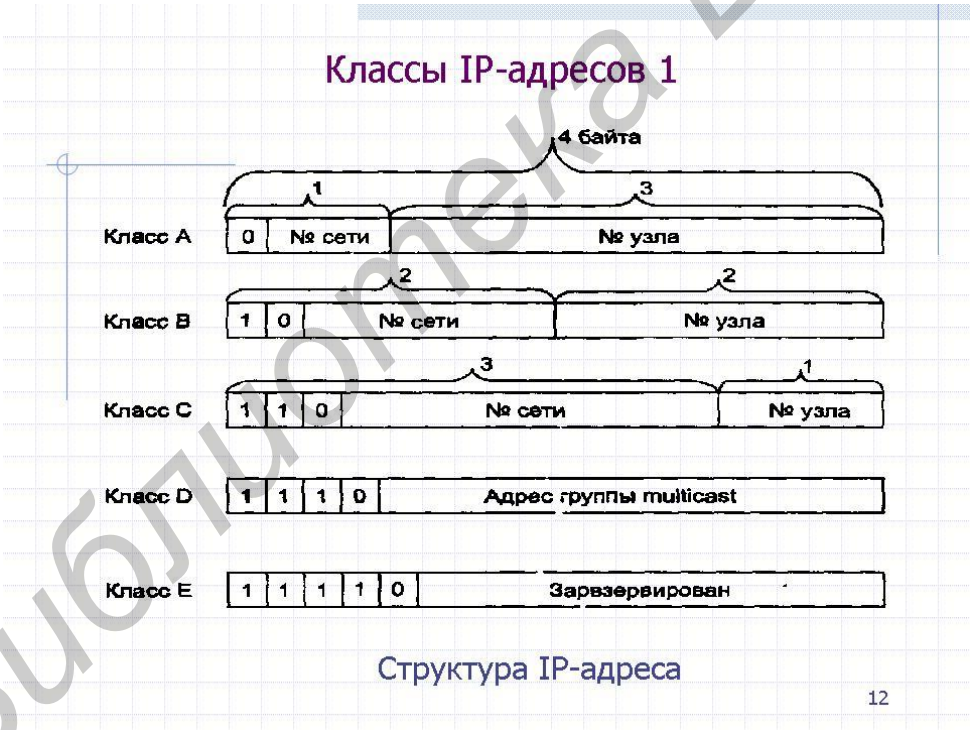
Пакет, направляемый адресату через составную сеть, имеет в заголовке IP-адрес назначения. По номеру сети назначения каждый очередной маршрутизатор находит IP-адрес следующего маршрутизатора.

10

Слайд 10. IP-адрес является составным: первая часть – это номер сети, вторая часть – номер узла этой сети.



Слайд 11. И номер сети, и номер узла содержатся в 4-байтном IP-адресе.



Слайд 12. Поля IP-адреса номера сети и номера узла разных классов содержат разное число двоичных разрядов, но сумма их равна 32 бита. Это сделано для более гибкой нумерации сетей разного размера.

Примерные цены IP-адресов

За последнее десятилетие цена IP-адресов лишь только увеличивалась.

Цена выставлявшихся на открытых торгах IP-адресов составляла следующие цифры:

- адрес класса C: не менее $10 000;
- адрес класса B: свыше $250 000;
- адрес класса A: свыше $64 000 000.

В силу такой дороговизны многие компании и частные лица не могут владеть собственными IP-адресами и поэтому арендуют их у своих поставщиков доступа в Internet.

13

Слайд 13. Ориентировочная цена IP-адресов разных классов.

Классы IP-адресов 2

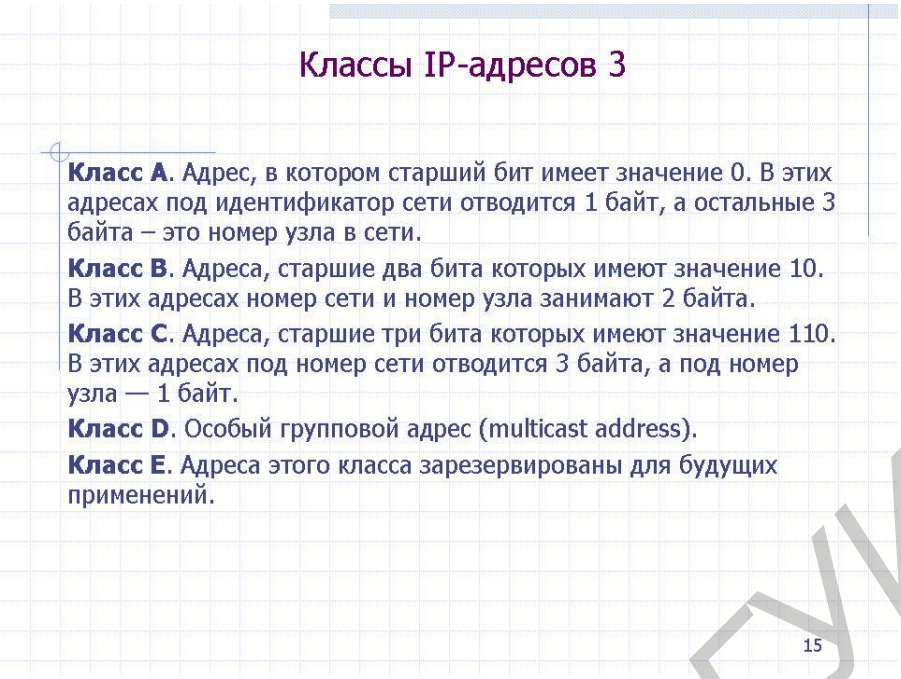
Характеристика IP-адресов разного класса

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0 (0 – не используется)	126.0.0.0 (127 – зарезервирован)	2^{24}, поле 3 байта
B	10	128.0.0.0	191.255.0.0	2^{16}, поле 2 байта
C	110	192.0.0.0	223.255.255.0	2^{8}, поле 1 байт
D	1110	224.0.0.0	239.255.255.255	Групповые адреса
E	11110	240.0.0.0	247.255.255.255	Зарезервировано

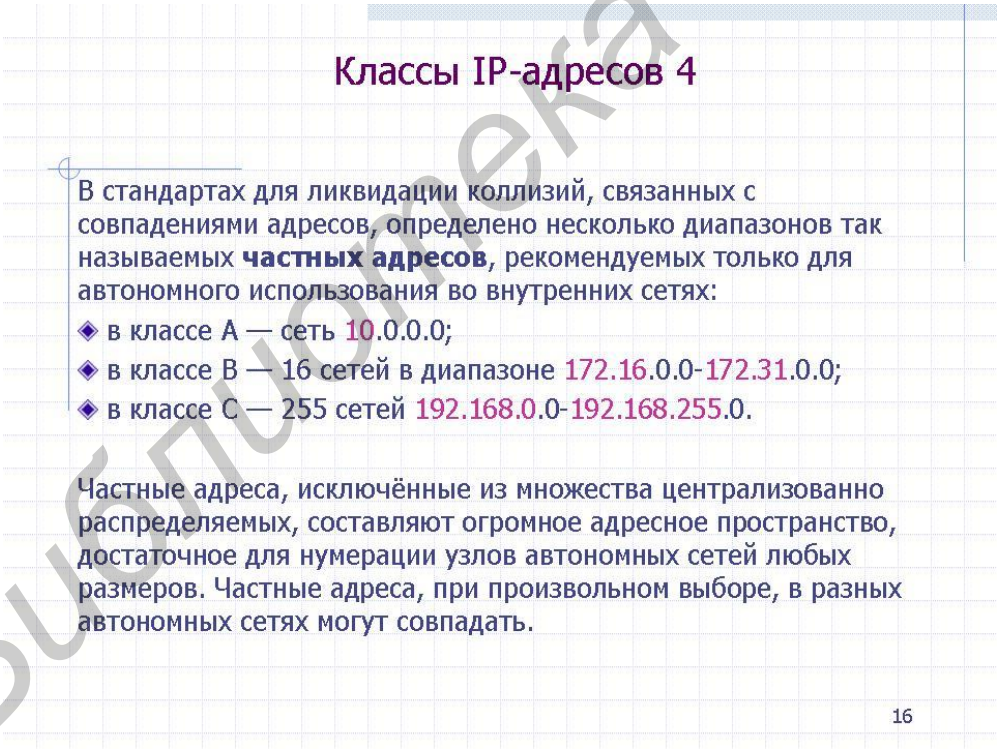
Классы IP-адресов

14

Слайд 14. Параметры и количество узлов в IP-адресах разных классов.



Слайд 15. Маски в старшем байте IP-адреса однозначно идентифицируют принадлежность соответствующей сети классу A, B, C или D.



Слайд 16. Три диапазона IP-адресов для каждого класса, не маршрутизируемые в глобальной сети, так называемые частные адреса.

Центральное распределение адресов 1

Уникальность сетевых адресов регулируется централизованной международной организацией ICANN (Internet Corporation for Assigned Names and Numbers), которая имеет региональные отделы:

- ARIN – Америка;
- RIPE – Европа;
- APNIC – Азия и Тихоокеанский регион.

Проблема распределения адресов, которая усугубляется нерациональным их использованием – их дефицит.

20

Слайд 17. Диапазоны IP-адресов по странам и континентам выделяют международные организации.

Центральное распределение адресов 2

На схеме показано соединение двух сетей глобальной связью. Видно нерациональное использование IP-адресов. Маршрутизаторы, используемые для связи, образуют вырожденную сеть, которая имеет отдельный номер сети и всего два узла.

21

Слайд 18. Жёсткая структура классов не позволяет использовать все значения из 32-битного диапазона для IP-адресов.

Центральное распределение адресов 3

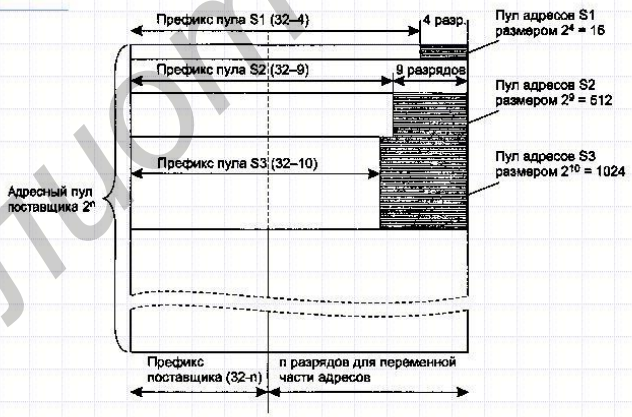
Для смягчения проблемы дефицита адресов существует несколько возможностей:

- переход на новую версию протокола IP – протокол IPv6, в котором адресное пространство расширено до 128 бит;
- оставаясь в рамках версии IPv4, более экономно расходовать существующие IP-адреса с помощью технологий NAT и CIDR.

22

Слайд 19. С развитием инфраструктуры сетей в планетарном масштабе номеров из 32-битного диапазона IP-адресов стало не хватать.

Адресация и технология CIDR 2



Поставщик имеет непрерывный диапазон адресов и распределяет их на основе технологии CIDR.

24

Слайд 20. Распределение IP-адресов по методу CIDR смягчило проблему дефицита адресов.

1.6 Лекция. Маршрутизация в IP-сетях

Объясняется работа IP-протокола на сетевом уровне, описывается заголовок IP-пакета. Разбирается простейшая схема маршрутизации и роль маршрутизатора. Приведены примеры таблиц маршрутизации и их построение. Разбирается алгоритм просмотра таблиц маршрутизации. Показан пример прохождения IP-пакетов через составную сеть.

Протокол IP относится к протоколам без установления соединения. Он поддерживает обработку каждого IP-пакета как независимой единицы обмена, не связанной с другими IP-пакетами. Этот протокол не имеет механизмов для обеспечения достоверности конечных данных. Основная функция протокола IP – маршрутизация как с масками, так и без использования масок. Этот протокол допускает и управляет фрагментацией пакетов.

1.6.1 Алгоритм просмотра таблиц маршрутизации без масок

Несмотря на разнообразие форматов таблиц маршрутизации, просмотр их подчинён жёсткому алгоритму, предписанному протоколом IP. При поступлении на один из интерфейсов маршрутизатора пакета IP-протокол извлекает из него адрес назначения, который обрабатывает по следующим правилам.

1. Выполняется **первая фаза** просмотра таблицы – поиск конкретного маршрута к узлу. IP-адрес последовательно строка за строкой сравнивается с содержимым поля адреса назначения таблицы маршрутизации. При совпадении из соответствующей строки извлекаются адрес следующего маршрутизатора и идентификатор выходного интерфейса. После этого просмотр таблицы завершается.

2. Если первая фаза окончилась неудачно и совпадения адресов не произошло, то протокол IP переходит ко **второй фазе** просмотра – поиску маршрута к сети назначения. Из IP-адреса вычленяется номер сети, и первое поле таблицы снова просматривается на предмет совпадения номера с номером сети из пакета. При совпадении из соответствующей строки таблицы извлекаются адрес следующего маршрутизатора и идентификатор выходного интерфейса, куда будет перенаправлен пакет на текущем маршрутизаторе. Просмотр таблицы на этом завершается.

3. При неудаче и в первой, и во второй фазе средствами протокола IP выбирается маршрут по умолчанию. Если маршрут по умолчанию отсутствует – пакет отбрасывается. Просмотр таблицы на этом заканчивается.

Последовательность фаз в данном алгоритме строго определена, в то время как упорядоченность расположения строк в таблице, включая запись о маршруте по умолчанию, никак не сказывается на результате.

1.6.2 Алгоритм просмотра таблиц маршрутизации с масками

Потребность в структуризации сетей в условиях дефицита нераспределённых номеров сетей требует применения дополнительных элементов в системе адресации узлов, позволяющих задействовать большее число сетей. Эти элементы, называемые масками, усложняют алгоритм маршрутизации, но позволяют достигнуть структуризации сетей и более эффективной их работы.

Просмотр таблиц, содержащих столбец маски, имеет много общего с алгоритмом просмотра таблиц, не содержащих маски. Есть и существенные различия.

1. Поиск маршрута для поступившего IP-пакета протокол начинает с того, что извлекает из него адрес назначения (обозначим его $IP_{Куда}$), затем просматривает всю таблицу маршрутизации. Просмотр таблицы маршрутизации осуществляется в два этапа.

2. Алгоритм осуществляет поиск **специфического маршрута** – это суть первого этапа.

С этой целью из каждой записи таблицы, по маске 255.255.255.255, извлекается адрес назначения и сравнивается с адресом из пакета $IP_{Куда}$. Если в какой-либо строке произошло совпадение, то адрес следующего маршрутизатора для пакета $IP_{Куда}$ берётся из этой строки.

3. Второй этап выполняется в случае, если специфический маршрут не найден. Тогда алгоритм ищет **неспецифический маршрут** к сети, к которой относится пакет с адресом $IP_{Куда}$. Протокол IP заново просматривает таблицу маршрутизации, и с каждой *i*-записью производит следующие действия:

а) маска (обозначим её M_i), содержащаяся в данной *i*-записи, «накладывается», осуществляя операцию конъюнкции, на IP-адрес узла назначения $IP_{Куда}$, извлечённый из пакета:

$IP_{Куда}$ & M_i = $IP_{Сеть}$;

б) полученное в результате конъюнкции число $IP_{Сеть}$ сравнивается со значением из **поля адреса назначения** этой же записи таблицы маршрутизации;

в) в случае **совпадения** строка помечается;

г) аналогично протокол IP просматривает строку за строкой всю таблицу, включая строку и о маршруте по умолчанию. Когда просмотр записей заканчивается, происходит переход к следующему шагу.

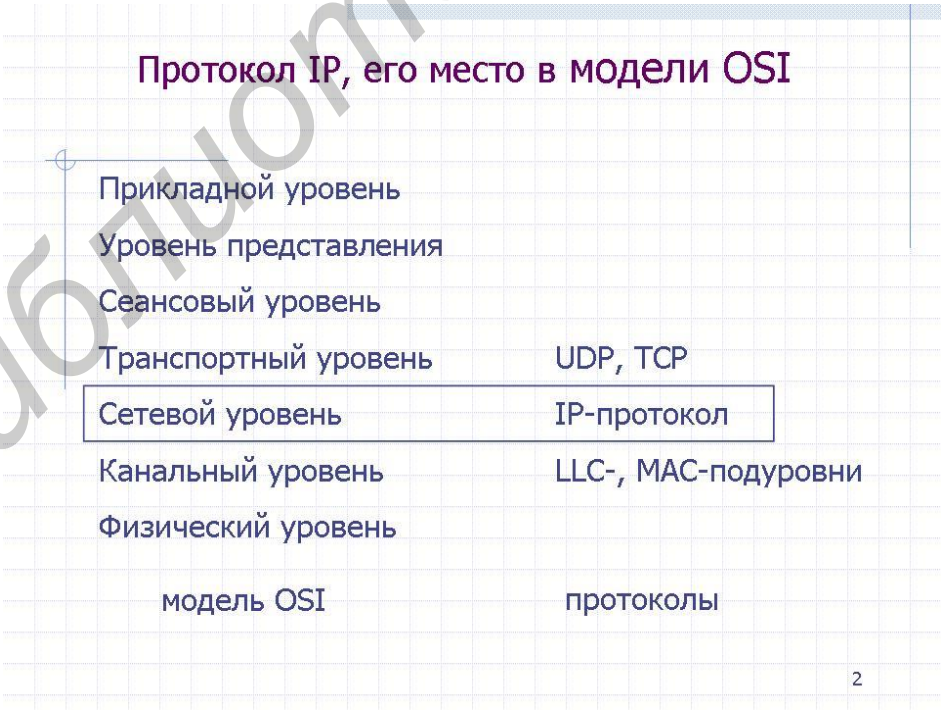
4. После просмотра всей таблицы:

1) если не произошло **ни одного** совпадения и маршрут по умолчанию отсутствует – пакет **отбрасывается**;

2) при **одном** совпадении пакет **отправляется по маршруту**, указанному в строке с совпавшим адресом;

3) в случае **нескольких** совпадений все помеченные строки сравниваются и выбирается тот маршрут, в котором количество совпавших разрядов наибольшее, то есть в случае принадлежности адреса $IP_{Куда}$ сразу нескольким сетям маршрутизатор использует наиболее **специфический маршрут**.

Во многих таблицах маршрутизации запись с адресом 0.0.0.0 и маской 0.0.0.0 соответствует маршруту по умолчанию. Действительно, любой адрес $IP_{Куда}$ в пришедшем пакете после наложения на него маски 0.0.0.0 даст адрес сети 0.0.0.0, что совпадает с адресом, указанным в записи. Поскольку маска 0.0.0.0 имеет нулевую длину, то этот маршрут считается **самым неспецифическим** и используется только при отсутствии совпадений с остальными записями из таблицы маршрутизации.



Слайд 1. Маршрутизация осуществляется IP-протоколом на сетевом уровне.

Протокол IP, формат IP-пакета

IP-пакет состоит из заголовка и поля данных.

Он имеет сложный заголовок, поскольку осуществляет функционально сложную обработку служебной информации.

Длина заголовка IP-пакета – 20 байт.

Он имеет следующие поля.

5

Слайд 2. IP-пакет устроен гораздо сложнее кадра Ethernet и содержит сложный заголовок.

Заголовок IP-пакета

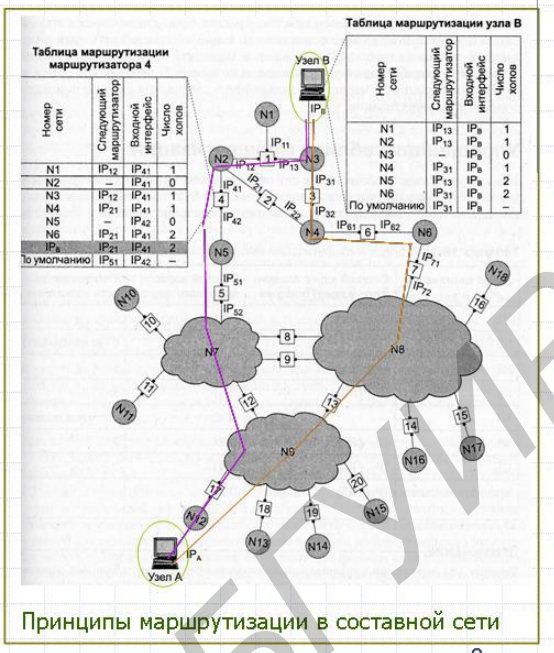
- номер версии – IPv4 или IPv6;
- длина заголовка – пять 32-битовых слов;
- тип сервиса (службы);
- полная длина фрагмента;
- идентификатор пакета;
- флаги;
- смещение сегмента;
- время жизни;
- протокол верхнего уровня;
- контрольная сумма заголовка;
- IP-адрес источника;
- IP-адрес приёмника.

6

Слайд 3. Поля заголовка IP-пакета.

Простейшая схема IP-маршрутизации

- Каждый маршрутизатор – это совокупность нескольких узлов.
- Маршрут выбирают маршрутизаторы и конечные узлы на основании имеющейся у них информации о конфигурации сети.
- Показана упрощённая таблица 4-го маршрутизатора и узла В.



Принципы маршрутизации в составной сети

8

Слайд 4. Схема простейшей маршрутизации в небольшой сети.

Поля таблицы маршрутизации

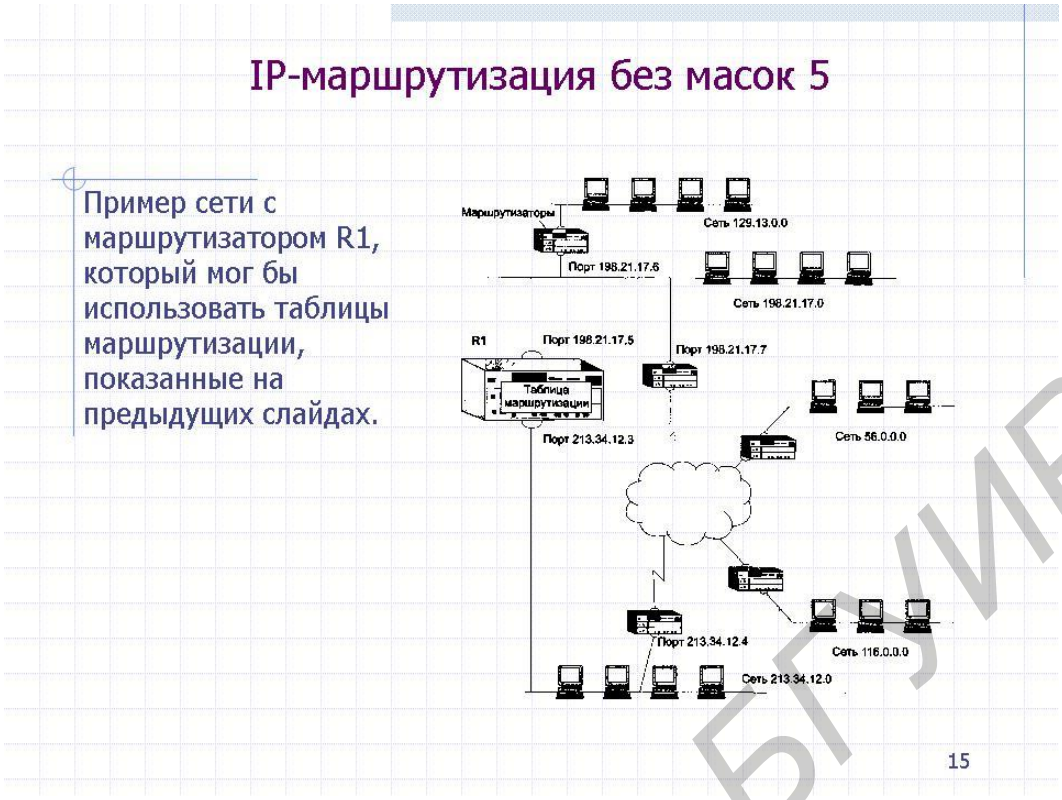
Назначение полей простейшей таблицы маршрутизации

1. Адрес назначения пакетов.
2. Сетевой адрес следующего маршрутизатора.
3. Сетевой адрес выходного порта.
4. "Расстояние" до сети назначения

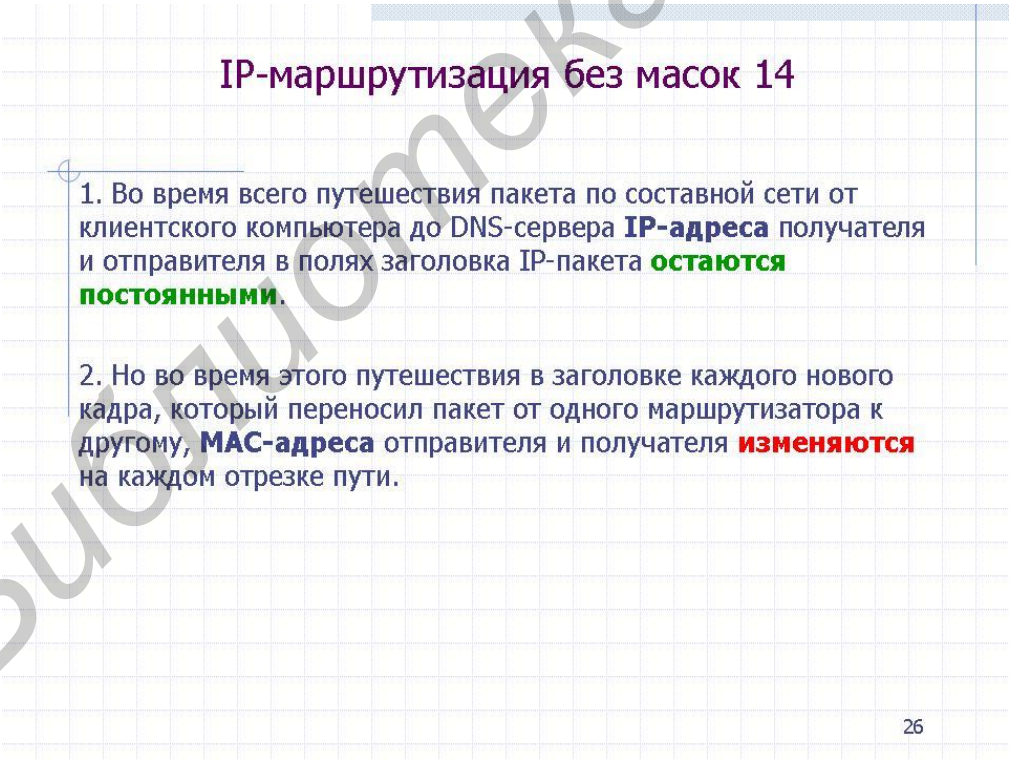
Если адрес сети отправляемого пакета не известен, он отправляется на маршрутизатор "по умолчанию".

9

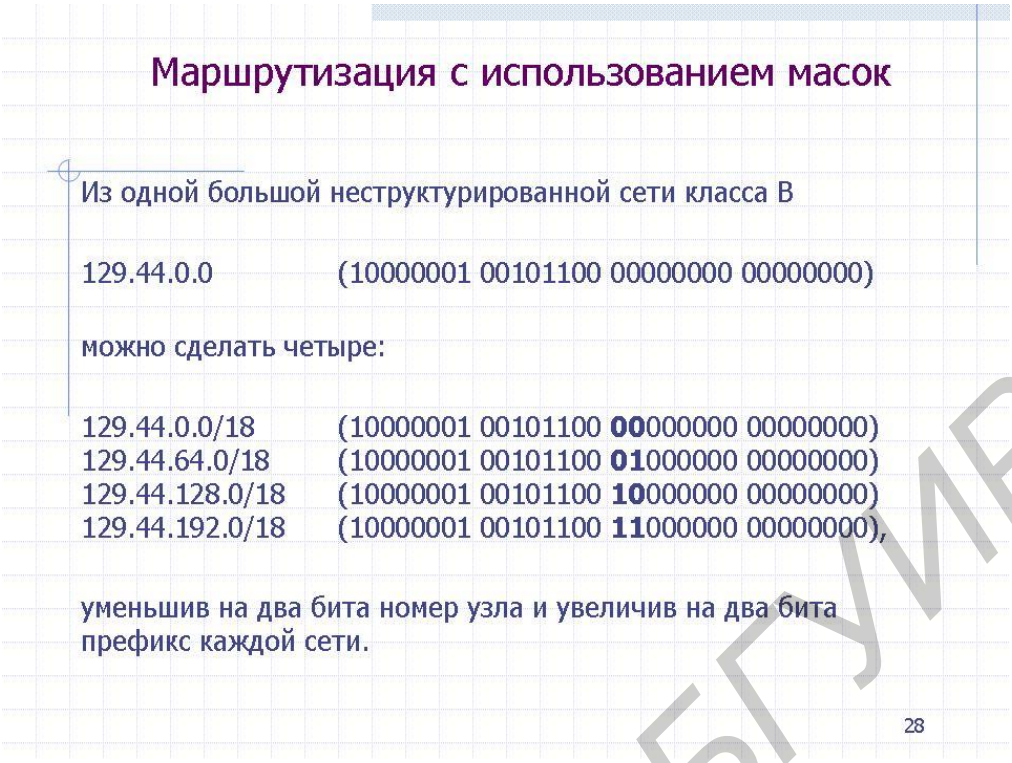
Слайд 5. Таблицы маршрутизации строятся по-разному, но у всех у них есть четыре регламентированных поля.



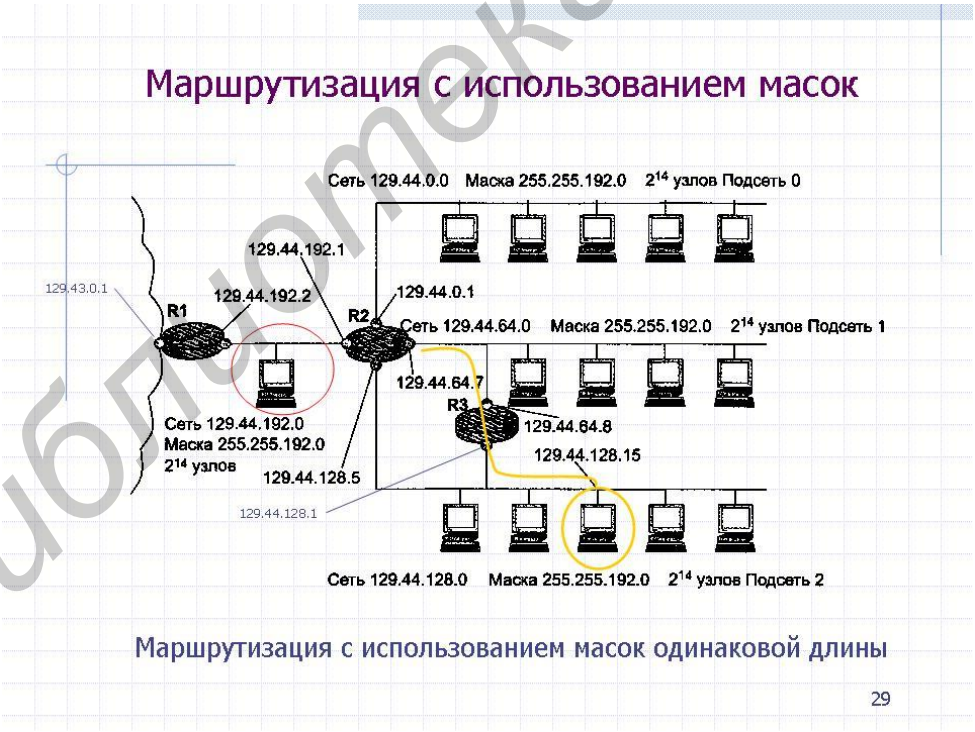
Слайд 6. Пример маршрутизации без масок.



Слайд 7. В процессе перепаковки IP-пакета на сетевом уровне его IP-адреса в заголовке не меняются.



Слайд 8. Стандартная процедура конъюнкции, используемая для вычленения номера сети из IP-адреса.



Слайд 9. Красным кружком обведена вырожденная сеть, поглотившая IP-адреса для 2^{14} хостов. Жёлтый путь – специфический маршрут.

Маршрутизация с использованием масок

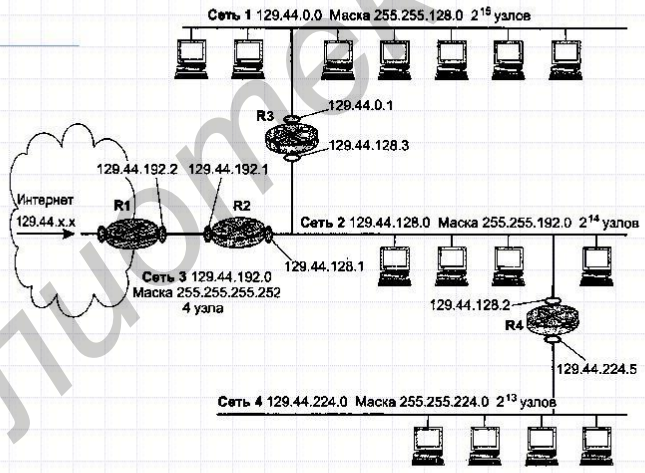
Адрес назначения	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.192.0	129.44.0.1	129.44.0.1	Подключена
129.44.64.0	255.255.192.0	129.44.64.7	129.44.64.7	Подключена
129.44.128.0	255.255.192.0	129.44.128.5	129.44.128.5	Подключена
129.44.192.0	255.255.192.0	129.44.192.1	129.44.192.1	Подключена
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	–
129.44.128.15	255.255.255.255	129.44.64.8	129.44.64.7	–

Таблица маршрутизатора R2 в сети с масками одинаковой длины

30

Слайд 10. При использовании масок в таблице маршрутизации появляется ещё одно обязательное поле – обведено зелёным.

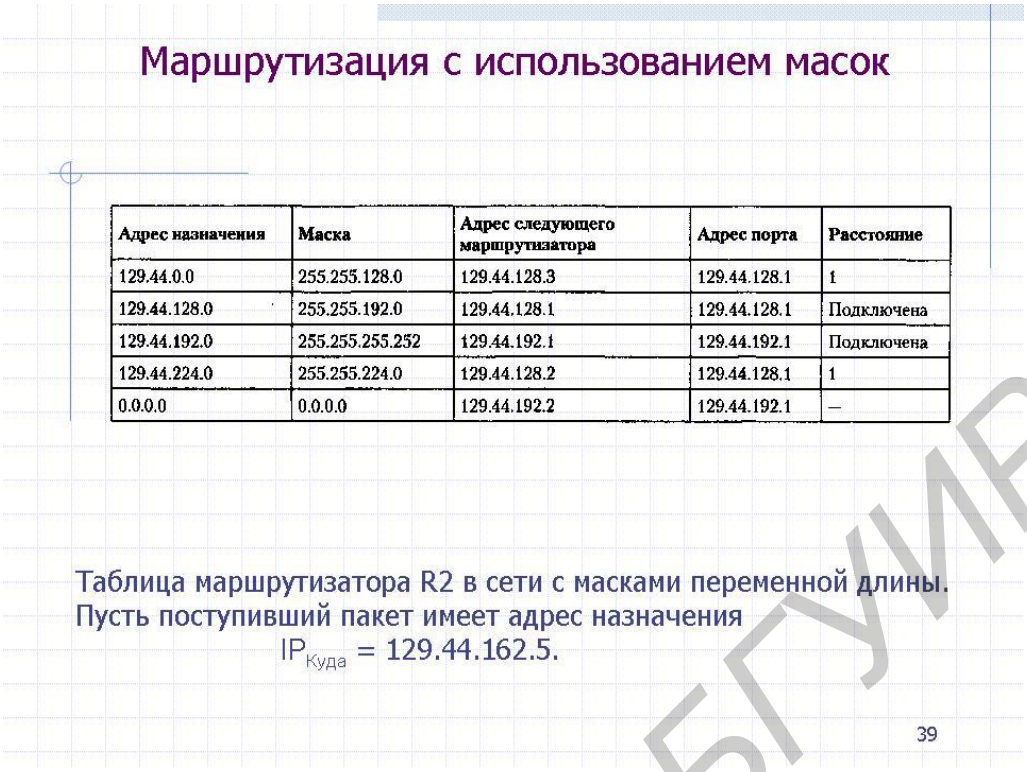
Маршрутизация с использованием масок



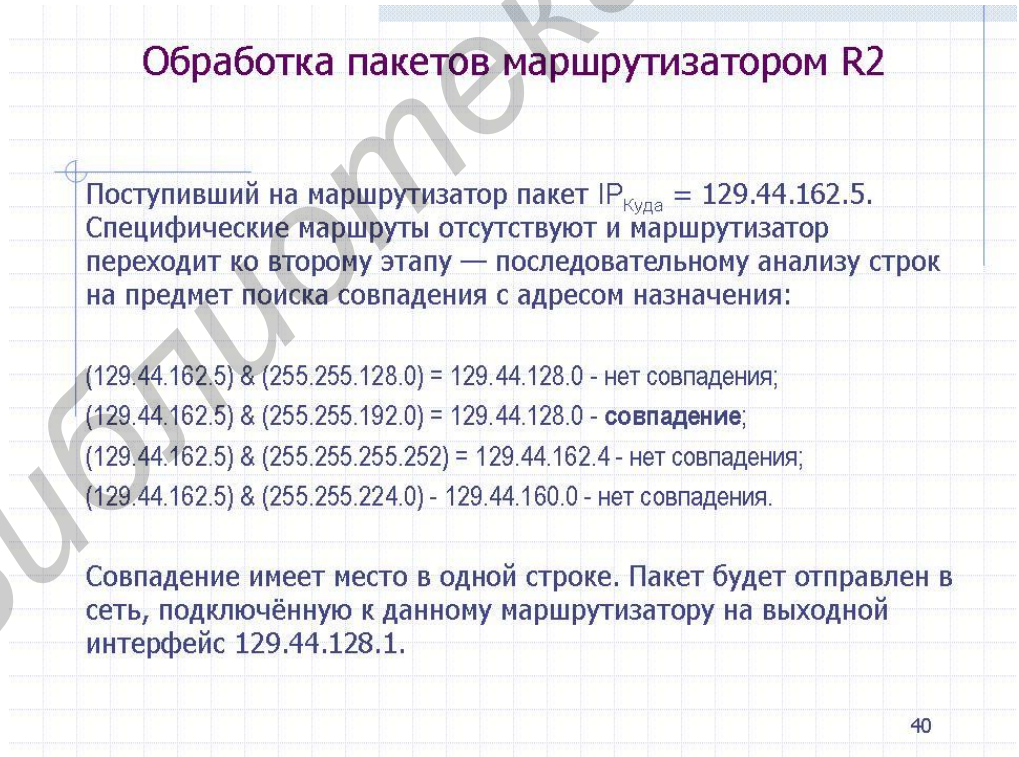
Структуризация сети масками переменной длины

38

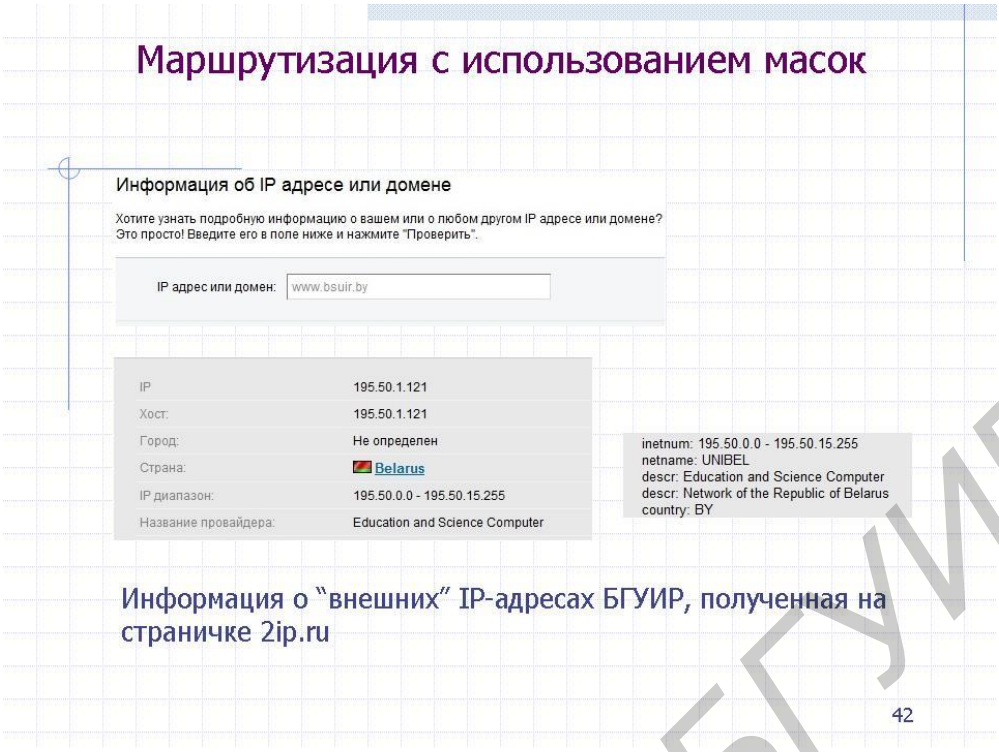
Слайд 11. С помощью масок переменной длины вырожденная сеть «схлопнулась», освободив дополнительные IP-адреса.



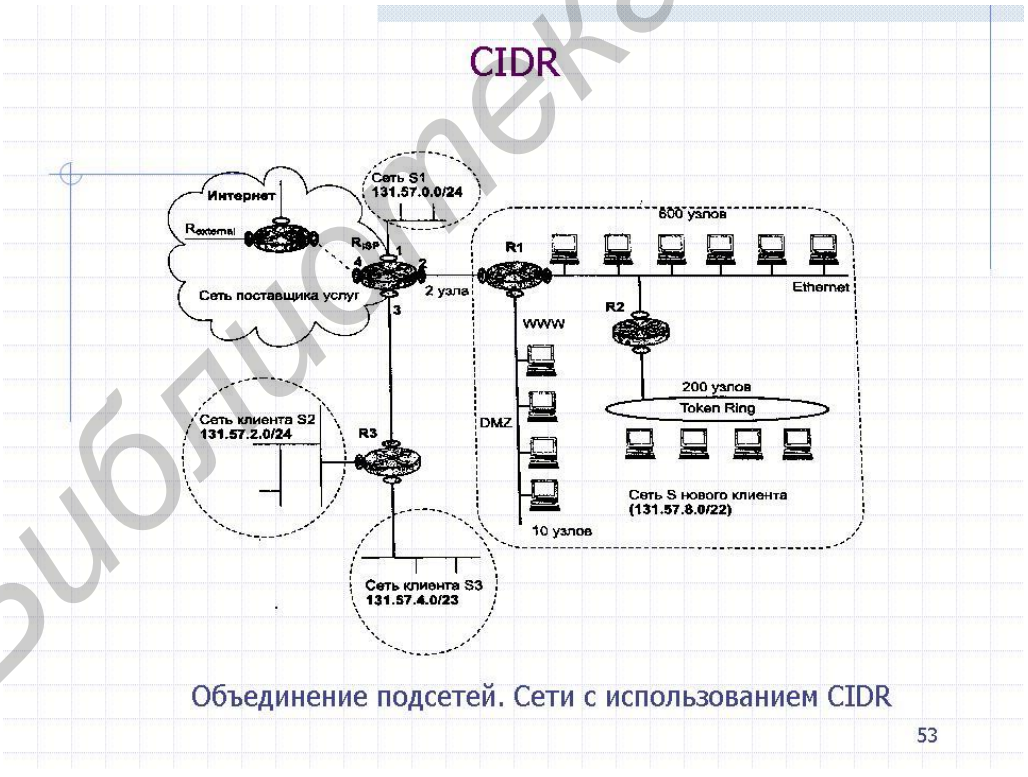
Слайд 12. Поучительный пример вычленения маршрутизатором номера сети из IP-адреса назначения.



Слайд 13. Использование конъюнкции для определения сети с помощью маски.



Слайд 14. Доступная информация о диапазоне IP-адресов сайта при его известном доменном имени.



Слайд 15. Использование CIDR для агрегации нескольких маленьких сетей.

Слайд 16. Агрегация CIDR на примере таблицы маршрутизации.

1.6.3 CIDR

При увеличении узлов в сети и несовершенстве протоколов маршрутизации обмен сообщениями об обновлении таблиц стал приводить к сбоям магистральных маршрутизаторов. Таблица магистрального маршрутизатора может содержать несколько тысяч маршрутов. С помощью масок сисадмин может **разделить** свою сеть на подсети.

Однако в процессе разделения на подсети с помощью масок проявляется обратный эффект их применения: теперь, для того чтобы направить весь суммарный трафик, адресованный из внешнего окружения в корпоративную сеть, разделённую на подсети, нам хотелось бы, чтобы во всех внешних маршрутизаторах наличествовала всего одна строка. В этой строке на месте адреса назначения должен быть указан общий префикс для всех этих сетей. Это осуществляется с помощью **бесклассовой междоменной маршрутизации** CIDR (Classless Inter-Domain Routing) [9].

Имеет место операция, обратная разделению на подсети, – операция агрегирования нескольких сетей в одну более крупную. К сожалению, распределение адресов носит во многом случайный характер. Кардинальный путь решения проблемы – перенумерование сетей. Однако эта процедура сопряжена с определёнными временными и материальными затратами.

Необходимым условием эффективного использования технологии CIDR является локализация адресов, то есть назначение адресов, имеющих совпадающие префиксы, сетям, располагающимся по соседству. В этом случае поток данных может быть агрегирован.

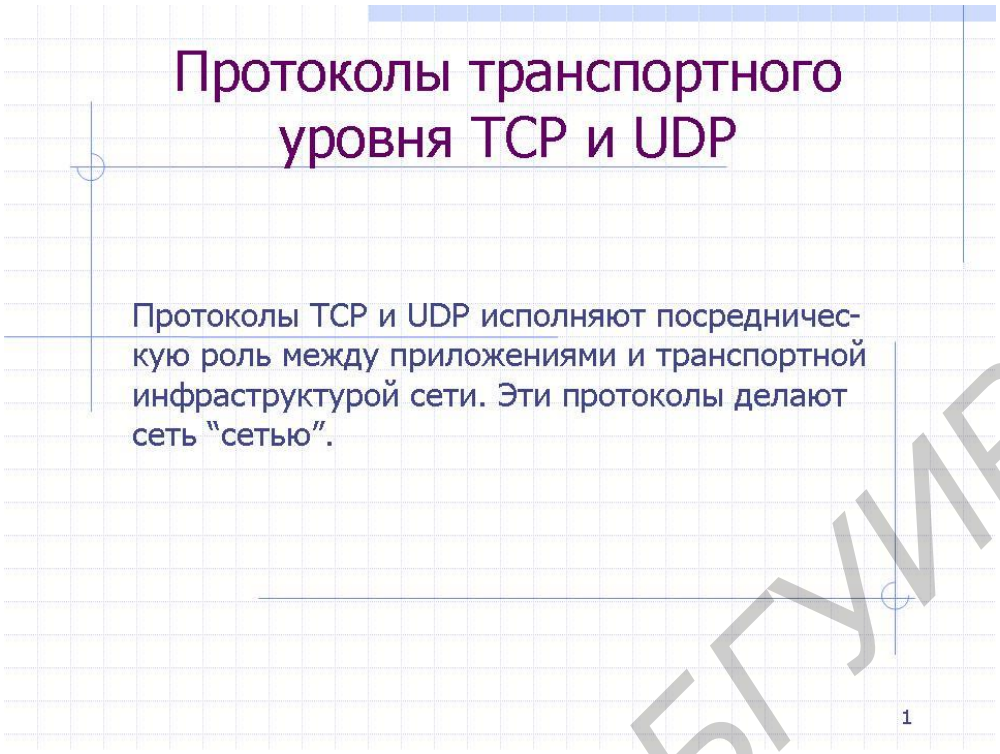
1.7 Лекция. Протоколы транспортного уровня TCP и UDP

В прошлой лекции 1.6 мы рассмотрели сетевое взаимодействие протокола IP, основная задача которого – передача данных между сетевыми интерфейсами в составной сети. Главная задача транспортного уровня, которую решают протоколы TCP и UDP, заключается в передаче данных между прикладными процессами, выполняющимися на компьютерах в сети.

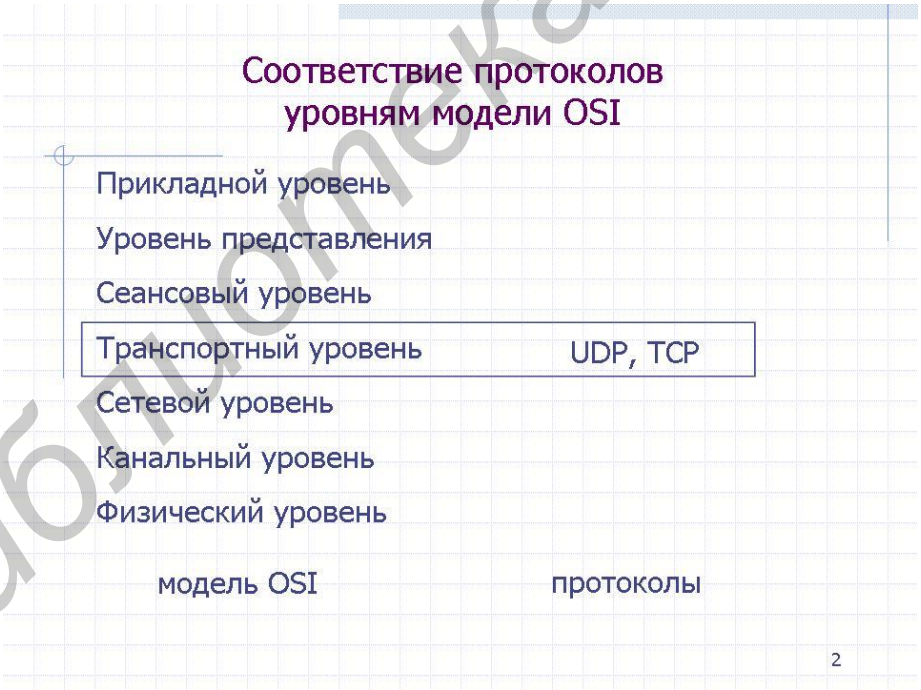
Эту задачу решают протоколы TCP и UDP на транспортном уровне, распределяя пакеты данных, поступающие с сетевого уровня, между прикладными процессами операционной системы. Эта задача называется **демультиплексированием**.

Протоколы TCP и UDP ведут для каждого приложения системную очередь данных, поступающих к нему из сети. Такие системные очереди называются **портами**, причём входная и выходная очереди одного приложения рассматриваются как один порт. Таким портам присваиваются номера. Разбирается понятие сокета как пары IP-адреса и порта.

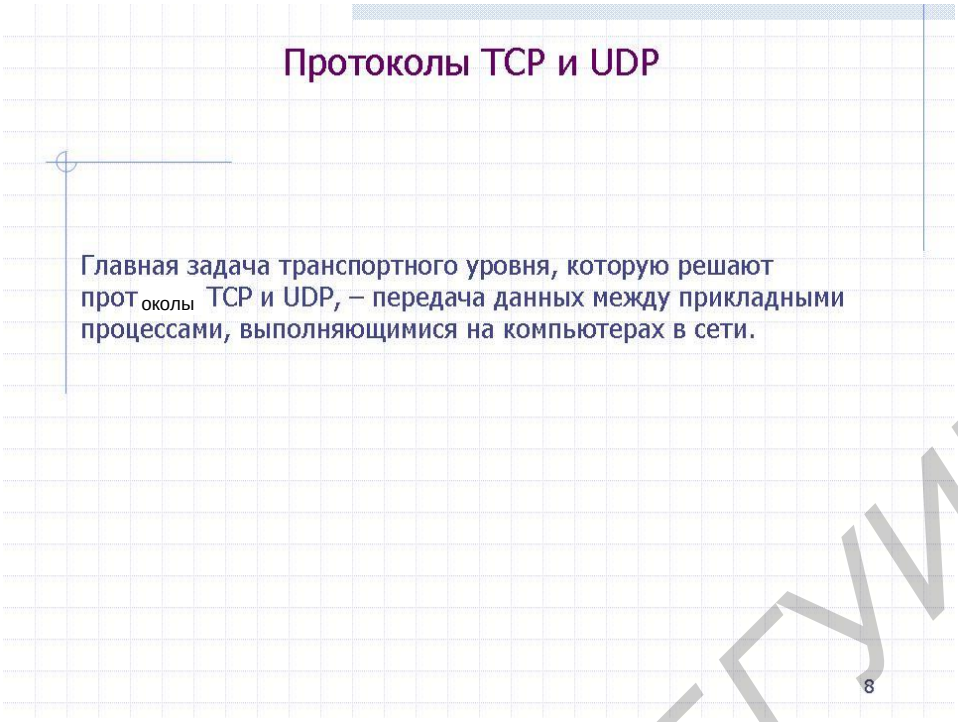
Рассматривается надёжный метод продвижения данных TCP с помощью установления логического соединения, квитирования и метода скользящего окна. Объясняется происхождение важнейших параметров скользящего окна: размера окна и времени тайм-аута.



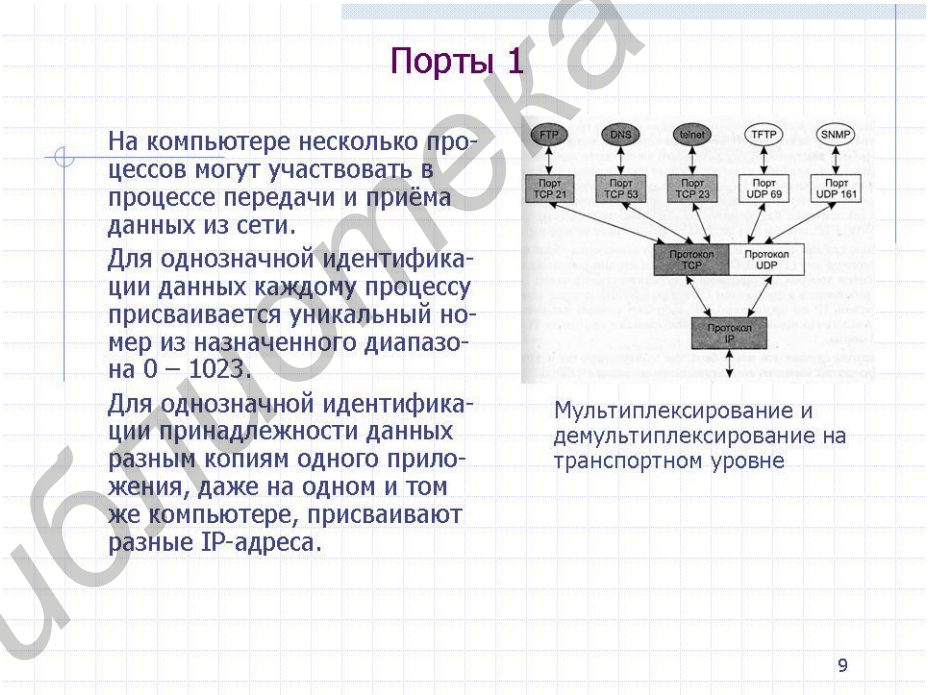
Слайд 1. Протоколы TCP и UDP – основа сети с коммутацией пакетов. Они расчленяют и «склеивают» данные при их пересылке.



Слайд 2. Протоколы TCP и UDP привязаны к транспортному уровню модели OSI.



Слайд 3. Протоколы TCP и UDP способны устанавливать логическое соединение, а протокол TCP отвечает за целостность данных.



Слайд 4. Протоколы TCP и UDP из одного потока информации, поступающего из сети, распределяют данные для различных процессов.

Порты 2

Протоколы TCP и UDP ведут для каждого приложения две системные очереди: очередь данных, поступающих к приложению из сети, и очередь данных, отправляемых этим приложением в сеть. Такие системные очереди называются портами.

Связка IP-адрес и номер порта называется сокетом (socket).

Сокет – программный объект, обычно системный, абстрагирующий точку доступа к транспортной системе. Сокет сопоставляется одному из портов одного из транспортных протоколов и служит удобной для прикладного программирования унифицированной надстройкой над ним.

5

Слайд 5. Заголовок TCP-сегмента не содержит IP-адреса для определения сокета. IP-адрес доставляет IP-протокол с сетевого уровня.

Порты 3

После обработки поступившего из сети IP-пакета и продвижении его наверх IP-заголовок отбрасывается, но вместе с содержимым поля данных на транспортный уровень передаётся и IP-адрес.

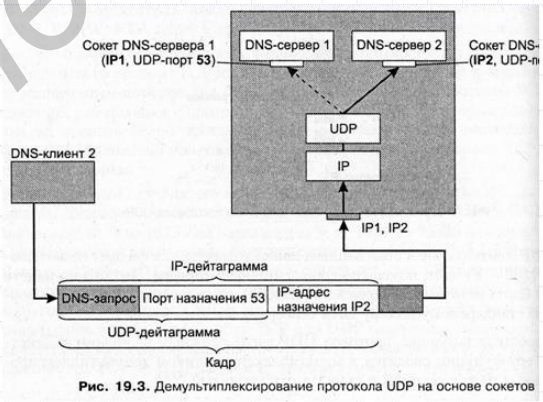


Рис. 19.3. Демультиплексирование протокола UDP на основе сокетов

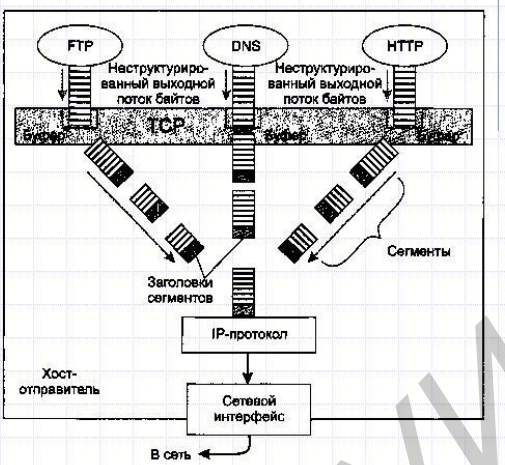
Демультиплексирование протокола UDP на основе сокетов, где для снятия неоднозначности в идентификации приложений, разные копии связываются с разными IP-адресами.

11

Слайд 6. Протоколы TCP и UDP могут иметь совпадающие номера портов (и IP-адресов), но сокеты у них будут всё равно разные.

Протокол TCP. 1

Данные поступают от нескольких процессов, которые буферизуются средствами TCP. Для передачи на сетевой уровень из них "вырезается" сегмент и снабжается заголовком.



Формирование TCP-сегментов из потока байтов

9

Слайд 7. Протокол TCP осуществляет уплотнение данных многих сетевых приложений в один поток IP-пакетов.

Протокол TCP. 2

Формат заголовка TCP-сегмента.

2 байта								2 байта
Порт источника (sours port)								**Порт приемника** (destination port)
Последовательный номер (sequence number) - номер первого байта данных в сегменте, определяет смещение сегмента относительно потока отправляемых данных								
Подтвержденный номер (acknowledgement number) - максимальный номер байта в полученном сегменте, увеличенный на единицу								
Длина заголовка (hlen)	**Резерв** (reserved)	URG	ACK	PSH	RST	SYN	FIN	**Окно** (window) - количество байтов данных, ожидаемых отправителем данного сегмента, начиная с байта, номер которого указан в поле подтвержденного номера
Контрольная сумма (checksum)								**Указатель срочности** (urgent pointer) - указывает на конец данных, которые необходимо срочно принять, несмотря на переполнение буфера
Параметры (options) - это поле имеет переменную длину и может вообще отсутствовать, используется для решения вспомогательных задач, например, для согласования максимального размера сегмента								
Заполнитель (paddind) - это фиктивное поле может иметь переменную длину, используется для доведения размера заголовков до целого числа 32-битовых слов								

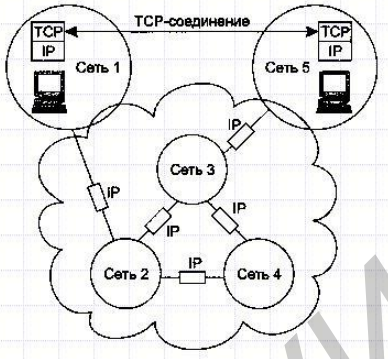
10

Слайд 8. Сложный и громоздкий заголовок сегмента TCP. TCP-протокол для своей работы требует много ресурсов компьютера.

Протокол TCP. 4

Логические соединения – основа надёжности TCP. Между двумя прикладными процессами создаётся виртуальное соединение.

В результате взаимодействия модулей TCP с двух сторон соединения определяются параметры соединения.



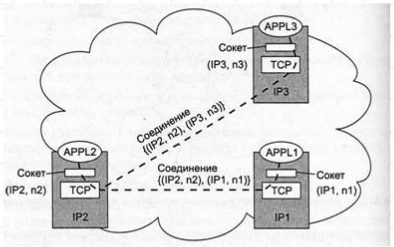
Соединение устанавливается по инициативе клиентской части приложения.

12

Слайд 9. Установленное логическое соединение отнюдь не эквивалентно соединению двух абонентов в телефонной сети.

Протокол TCP. 7

Логическое TCP-соединение однозначно идентифицируется парой сокетов. Благодаря логическому соединению вероятность потерять сегменты данных уменьшается.



Оба соединения установленно одним сокетом (IP2, n2)

24

Слайд 10. TCP-протокол может устанавливать несколько логических соединений одновременно.

Протокол TCP. Квитирование с ожиданием 1

Организация надёжной передачи – это создание потока квитанций. В протоколе TCP используется частный случай квитирования — алгоритм скользящего окна, который достаточно сложен в реализации.

Более простая схема обмена квитанциями – метод простоя источника (или квитирование с ожиданием), при котором источник не передаёт следующий сегмент, не дождавшись подтверждения – квитанции.

Если же квитанция в течение тайм-аута не пришла, то сегмент (или квитанция) считается утерянным и его передача повторяется.

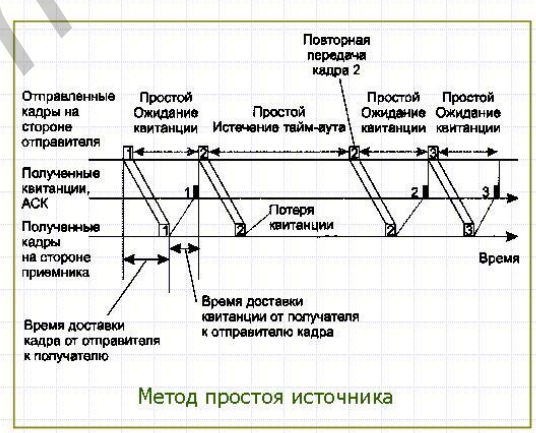
26

Слайд 11. TCP-протокол должен уметь различать и удалять повторные сегменты, посылаемые ему в результате утери квитанции.

Протокол TCP. Квитирование с ожиданием 2

При таком алгоритме работы источника принимающая сторона должна уметь распознавать дублирующиеся сегменты и избавляться от них.

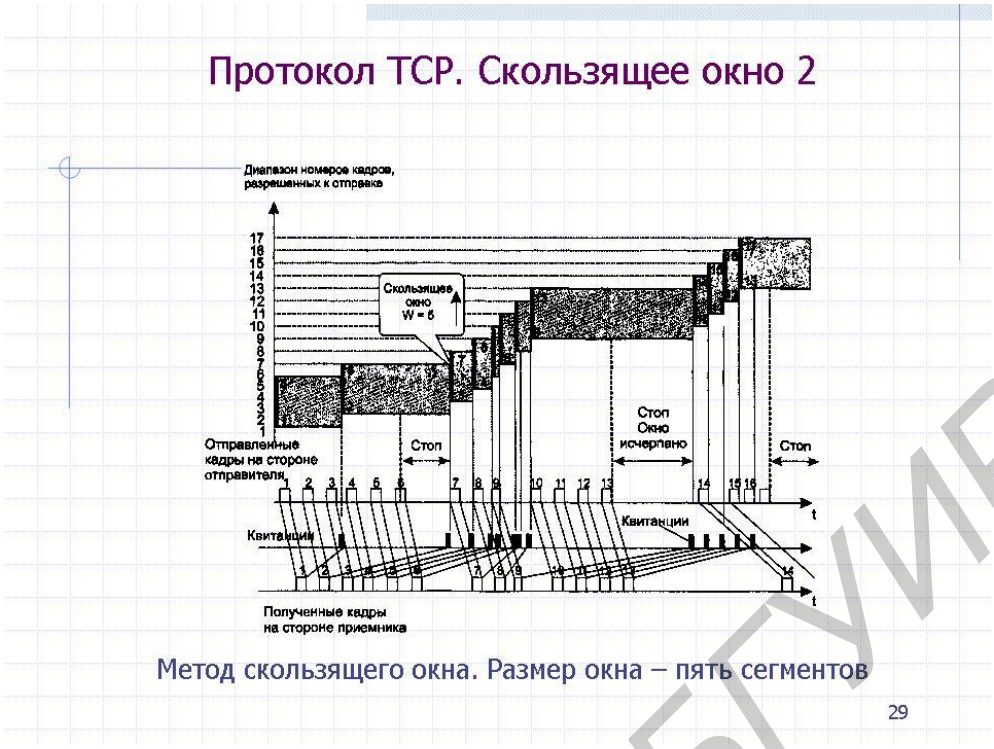
При использовании метода простоя источника производительность обмена данными ниже потенциально возможной.



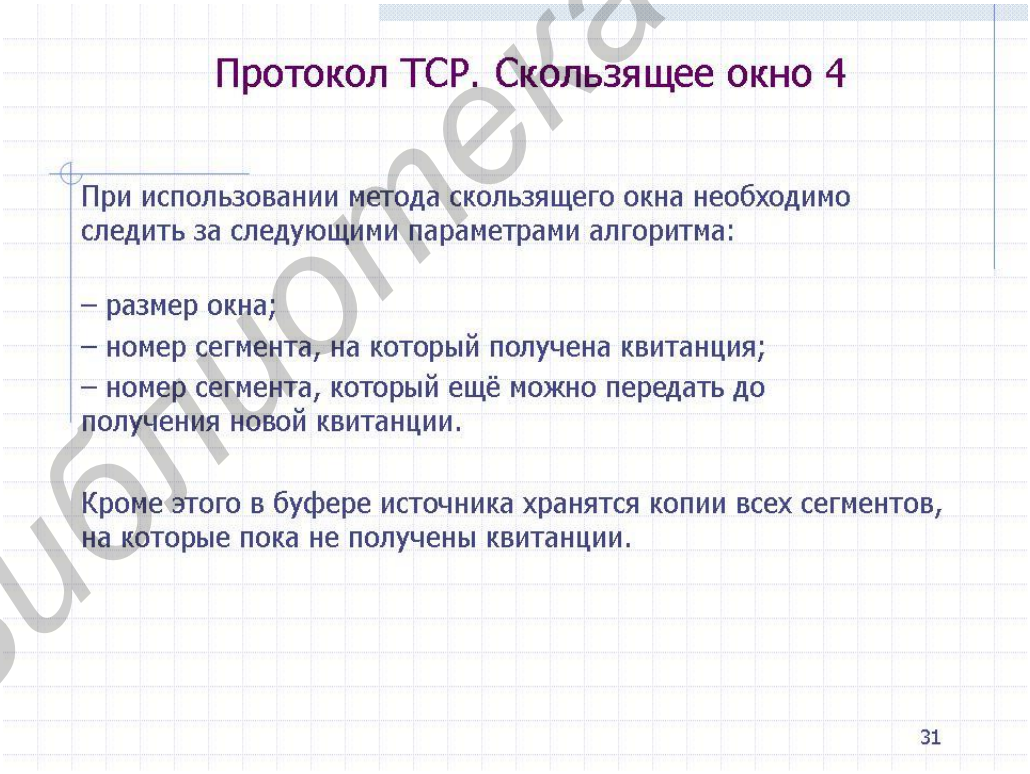
Метод простоя источника

27

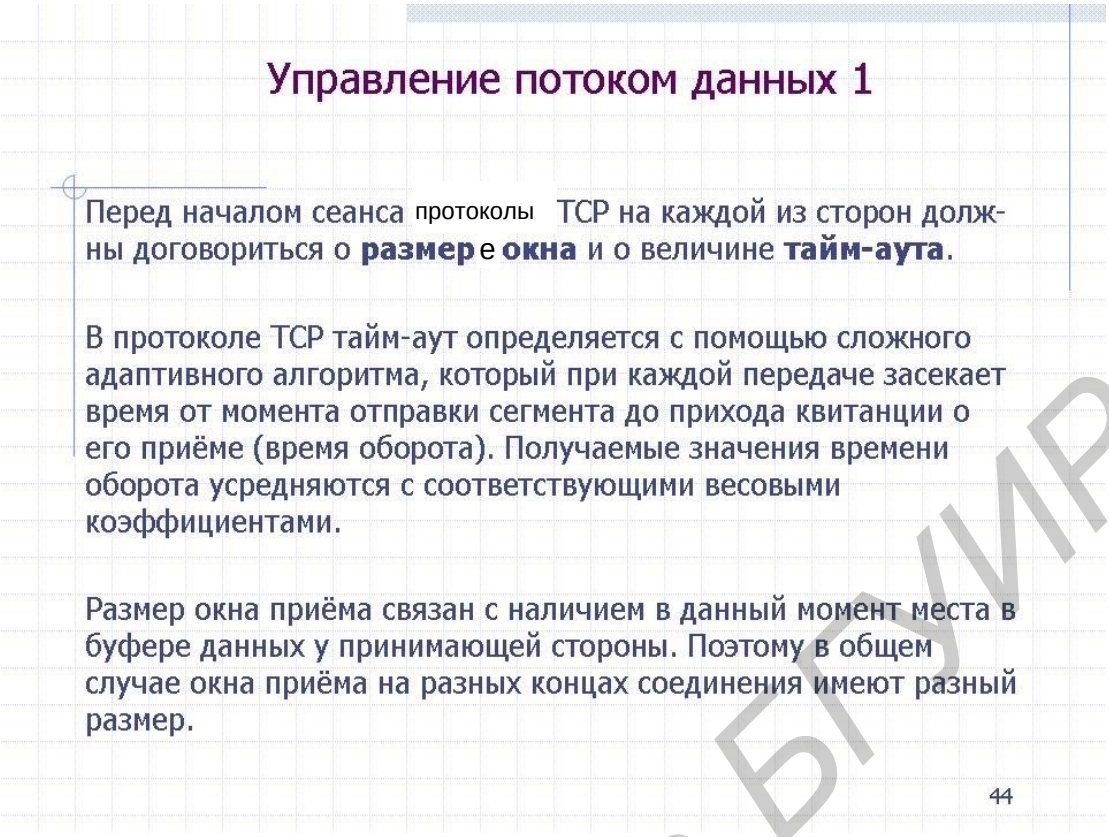
Слайд 12. Метод простоя источника – простейшая схема скользящего окна.



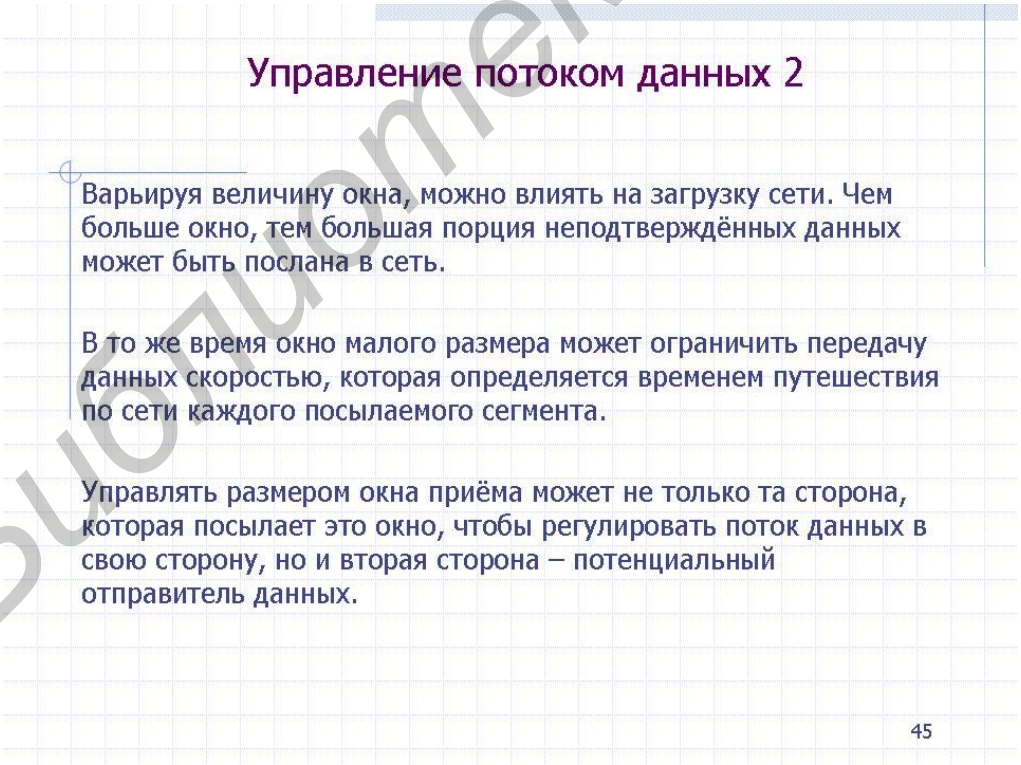
Слайд 13. Временная диаграмма отправки сегментов методом скользящего окна.



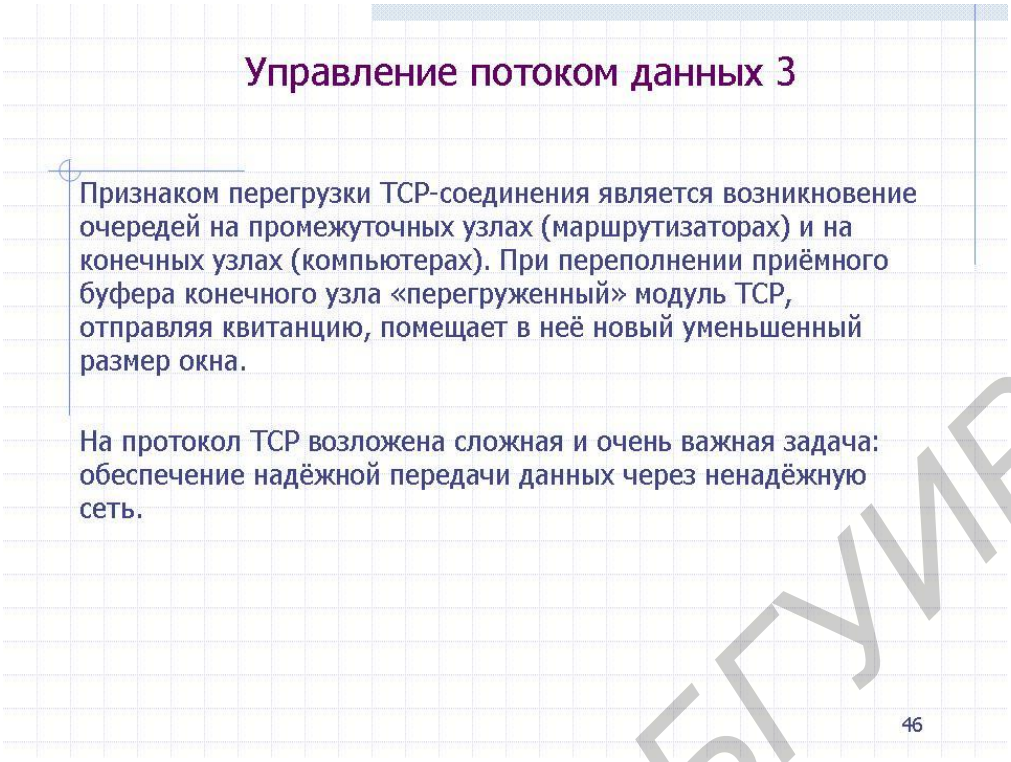
Слайд 14. Основные параметры скользящего окна, необходимые для правильной работы протокола TCP.



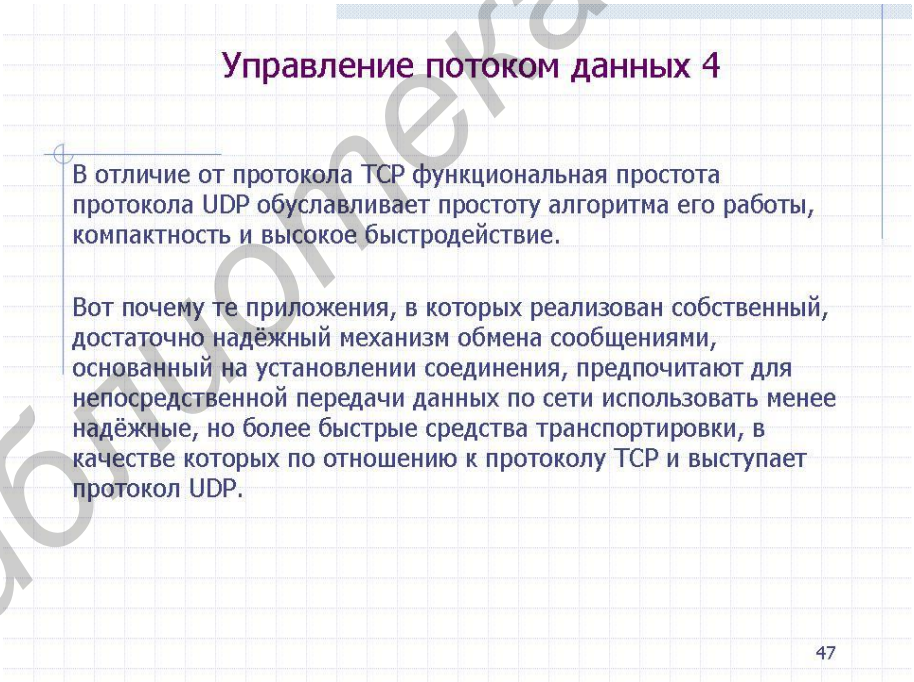
Слайд 15. Алгоритм, используемый протоколом TCP для установки размера скользящего окна и величины тайм-аута.



Слайд 16. Динамика изменения величины скользящего окна от скорости передачи и загруженности сети.



Слайд 17. Динамика изменения величины скользящего окна при перегруженности сети.



Слайд 18. Легковесный UDP как альтернатива тяжеловесному протоколу TCP.

1.8 Лекция. Удалённый клиентский доступ

Термин «удалённый доступ» (remote access) часто употребляют, когда речь идет о доступе пользователя домашнего компьютера к Интернету или сети предприятия, которая находится от него на значительном расстоянии, означающем необходимость применения глобальных связей. В последнее время под удалённым доступом стали понимать не только доступ изолированных компьютеров, но и домашних сетей, объединяющих несколько компьютеров членов семьи. Такими же небольшими сетями располагают малые офисы предприятий, насчитывающие 2-3 сотрудника.

Организация удалённого доступа является одной из наиболее острых проблем компьютерных сетей в настоящее время. Она получила название «проблемы последней мили», где под последней милей подразумевается расстояние от точки присутствия (POP – Point Of Present) оператора связи до помещений клиентов. Сложность этой проблемы определяется несколькими факторами. С одной стороны, современным пользователям необходим высокоскоростной доступ, обеспечивающий качественную передачу трафика любого типа, в том числе данных, голоса, видео. Для этого нужны скорости в несколько мегабит, а для качественного приема телевизионных программ – в несколько десятков мегабит в секунду. С другой стороны, подавляющее большинство домов в больших и малых городах и особенно в сельской местности по-прежнему соединены с точками присутствия операторов связи абонентскими окончаниями телефонной сети, которые не были рассчитаны на передачу компьютерного трафика.

Долгое время наиболее распространенной технологией доступа был коммутируемый доступ, когда пользователь устанавливал коммутируемое соединение с корпоративной сетью или Интернетом через телефонную сеть с помощью модема, работающего в голосовой полосе частот. Такой способ обладает существенным недостатком – скорость доступа ограничена несколькими десятками килобит в секунду из-за фиксированной узкой полосы пропускания примерно в 3,4 кГц, выделяемой каждому абоненту телефонной сети. Такие скорости сегодня устраивают все меньше и меньше пользователей.

Для организации скоростного удалённого доступа сегодня привлекаются различные технологии, в которых используется только существующая инфраструктура абонентских окончаний – телефонные сети или сети кабельного телевидения. После достижения POP поставщика услуг по такому окончанию компьютерные данные

уже не следуют по телефонной сети или сети кабельного телевидения, а ответвляются с помощью специального оборудования в сеть передачи данных. Это позволяет преодолеть ограничения на полосу пропускания, отводимую абоненту в телефонной сети или сети кабельного телевидения, и повысить скорость доступа. Наиболее популярными технологиями такого типа являются технология ADSL, использующая телефонные абонентские окончания, и кабельные модемы, работающие поверх сети кабельного телевидения. Эти технологии обеспечивают скорость от нескольких сотен килобит до нескольких десятков мегабит в секунду. Применяются также различные беспроводные технологии доступа, обеспечивающие как фиксированный, так и мобильный доступ. Набор таких беспроводных технологий очень широк.

1.8.1 Схемы удалённого доступа и типы абонентских окончаний

Удалённый доступ к сети представляет из себя разнообразный набор сетевой аппаратуры клиентов и операторов связи, а также смесь различных сетевых идеологий и протоколов.

Клиентов, использующих удалённый доступ к компьютерной сети, обычно подразделяют по типу подключённой аппаратуры и предполагаемого объёма трафика:

- пользователи с одним компьютером (иногда телефон и телевизор);
- пользователи с двумя абонентскими окончаниями – телефон и кабельное телевидение;
- пользователи, не имеющие проводного абонентского окончания и желающие получить беспроводной доступ к сети, например через мобильный телефон;
- пользователи, имеющие небольшую локальную сеть, – небольшой офис или частное лицо.

Для передачи данных по какому-либо абонентскому окончанию поставщик услуг должен обеспечить передачу через это окончание компьютерных данных и совместить её с передачей информации, для которой это окончание было спроектировано, например с аналоговым телефоном или кабельным телевидением.

Кроме этого, клиенты могут быть подключены к разным поставщикам услуг и операторам связи. Для согласованной работы таких клиентов с компьютерной сетью все поставщики должны как-то взаимодействовать между собой для обслуживания таких клиентов.

Из приведенного выше мы видим: большинство клиентов используют либо телефонную линию, либо кабельное телевидение. Поэтому для обеспечения клиентов тремя основными на сегодня видами доступа (телефон – компьютер – телевизор) необходимо реализовать одновременную передачу информации разного типа по одной линии связи, то есть совместить передачу данных голоса, компьютера и телевизора. Хорошо бы использовать единственное абонентское окончание, способное передавать информацию всех трёх типов. Витая пара на эту роль не подходит, так как её полоса пропускания на расстояниях в несколько километров не превышает 1 МГц.

Во всех перечисленных способах доступа требуется мультиплексирование двух или всех трёх упомянутых типов информации на абонентском окончании. Помимо этого существуют различные способы беспроводного доступа, обеспечивающие передачу телевизионного сигнала и компьютерных данных в одном абонентском окончании. Исключением является только наиболее старый метод коммутируемого доступа, при котором аналоговое абонентское окончание может использоваться телефоном или модемом компьютера только попеременно.

Чаще всего в абонентском окончании для экономного и рационального использования линии связи используется метод частотного уплотнения, предполагающий выделение своей полосы частот для каждого устройства.

К примеру:

– телефонное соединение 4 кГц;
– компьютерные данные 10 МГц;
– кабельному телевидению 6 МГц.

Распределение полос передачи данных по оси частот показано на рисунке 1. Полоса частот, отведенная для компьютерных данных, разделена на неодинаковые части. Это связано с разными потоками данных к компьютеру пользователя большого **входящего трафика** (download) и маленького **исходящего** (upload).

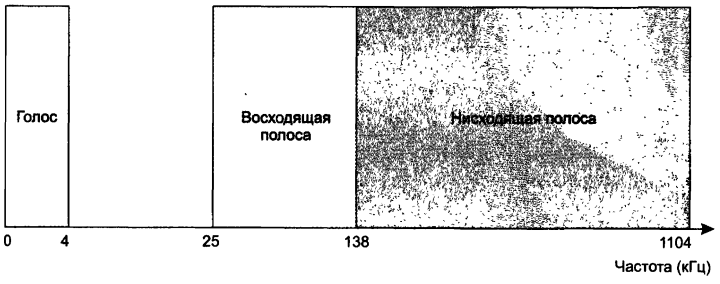


Рисунок 1 – Расположение источников данных на шкале частот

При реализации мультиплексирования в точках присутствия у клиента устанавливают распределители, которые и осуществляют эти функции. Распределитель чаще всего представляет собой пассивный полосовой фильтр*, который выделяет сигнал из нужного диапазона частот и передаёт его на отдельный выход, к каждому терминальному устройству абонента: телефону, телевизору и компьютеру. Компьютер использует дискретные сигналы для обмена данными, и поэтому для него требуется дополнительное устройство, преобразовывающее дискретные сигналы в аналоговые.

Несколько лет назад закончилась эра недорогих коммутируемых, так называемых dial-up, модемов, которые имел, наверно, каждый пользователь домашнего компьютера. Такой модем работал со стандартной полосой частот – 4 кГц – в аналоговых телефонных сетях. Dial-up модем не разделяет эту полосу ни с каким другими устройством, целиком занимая её для передачи компьютерных данных. Полосовой фильтр в этом случае не нужен.

Dial-up модемы остались в прошлом. Какие же оконечные устройства для компьютерных данных имеются у пользователя в точке присутствия сейчас? Их два: ADSL-модем (Assymetric Digital Subscriber Line) и кабельный модем. Первый работает на абонентских окончаниях телефонных сетей, а второй – в кабельном телевидении. Для этих устройств уже необходим полосовой фильтр, так как на эти оконечные устройства вместе с компьютерными данными по соседней полосе частот передаются телефонные и телевизионные сигналы.

Как обстоит дело с подключением оконечных устройств на стороне пользователя? К поставщику по кабелю поступает тоже смесь телефонных, компьютерных и телевезионных сигналов, у поставщика тоже установлены соответствующие полосовые фильтры, которые разделяют эту смесь сигналов, и каждый из них направляется на соответствующее оборудование.

В результате телефонные сигналы поступают на телефонный коммутатор поставщика и далее передаются в телефонную сеть. Телевизионные сигналы собираются на телевизионном оборудовании и, наконец, компьютерные данные поступают на устройство, концентрирующее компьютерный трафик и передающее его в локальную сеть поставщика услуг. Это устройство (рисунок 2) часто называют сервером удалённого доступа RAS (Remote Access Server).

---

* В настоящее время для названия “полосовой фильтр” в околокомпьютерном сообществе укореняется слово “сплиттер” – калька с английского splitter – расщепитель.

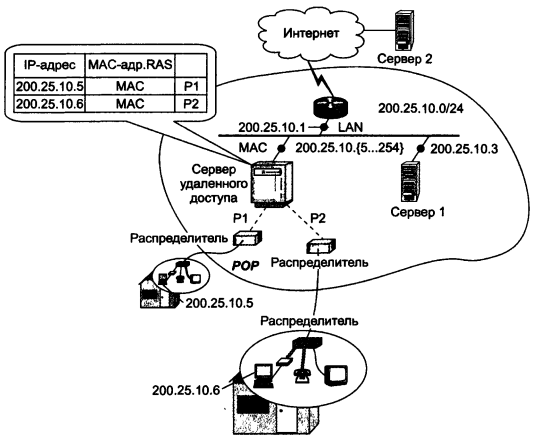


Рисунок 2 – Организация удалённого доступа

Сервер удалённого доступа содержит большое количество модемов, которые выполняют обратные операции по отношению к модемам пользователей. Помимо модемов, RAS подключён к маршрутизатору, который собирает трафик от пользователей и передаёт его в локальную сеть поставщика. Из этой локальной сети трафик передаётся обычным способом в Интернет или в определённую корпоративную сеть.

Рассмотренная схема доступа в зависимости от выбранного типа абонентского окончания и типа модема требует различных технологий. Но в терминах модели OSI все они являются технологиями **физического уровня**, так как создают поток битов между компьютером клиента и локальной сетью поставщика услуг. Для работы протокола IP поверх этого физического уровня должен использоваться один из протоколов канального уровня. Наиболее часто при удалённом доступе применяется протокол PPP, который поддерживает функцию назначения IP-адресов клиентскому компьютеру и аутентификацию пользователя.

1.8.2 Коммутируемый аналоговый доступ

Компьютер пользователя подключается к телефонной сети с помощью коммутируемого модема, который поддерживает стандартные процедуры набора номера и имитирует работу телефонного аппарата для установления соединения с RAS. Коммутируемый доступ может быть аналоговым или цифровым в зависимости от типа абонентского окончания сети. Рассмотрим обе эти возможности.

В телефонных сетях связь между абонентами осуществляется в основном аналоговыми сигналами, что позволяет пользоваться теми же сравнительно простыми и недорогими аналоговыми телефонными аппаратами, что и сто лет назад.

Телефонная сеть образована некоторым количеством коммутаторов, соединёных между собой цифровыми каналами. Топология связей между телефонными коммутаторами носит произвольный характер, но часто имеет место многоуровневая иерархия, когда несколько коммутаторов нижнего уровня подключаются к коммутатору более высокого уровня.

Обычно длина абонентского окончания не превышает 1-2 км, однако иногда оператор вынужден использовать и более протяжённые окончания, до 5-6 км, если имеется несколько удалённых абонентов.

Телефонная сеть, как сеть с коммутацией каналов, требует обязательной процедуры предварительного установления соединения между абонентскими устройствами. После этого в сети устанавливается канал между абонентами, через который они могут вести разговор. Установление соединения осуществляется с помощью сигнального протокола. В аналоговых телефонных сетях абоненту выделяется полоса частот шириной в 4 кГц. Из этой полосы 3,1 кГц предназначается для передачи собственно голоса, а оставшиеся 900 Гц служат для передачи сигнальной информации между аналоговыми коммутаторами.

Для получения доступа в Интернет через телефонную сеть нужен прибор, называемый модемом (**мо**дулятор-**де**модулятор). Модем пользователя должен выполнить вызов по одному из номеров, сообщённых провайдером, который соединяет его с сервером удалённого доступа. После установления соединения между модемами в телефонной сети образуется канал с полосой пропускания, не превышающей 4 кГц. Такая ширина полосы – принципиальное ограничение на скорость передачи данных коммутируемого модемного соединения.

Наивысшим достижением скорости передачи данных Dial-up-модемом является 56 кбит/с при использовании последней версии протокола V.90. Развивать дальше это семейство протоколов оказалось бессмысленным, поскольку, во-первых, был достигнут теоретический предел скорости передачи данных для ширины полосы 4 кГц в телефонных линиях, во-вторых, были разработаны новые, более эффективные способы передачи данных через те же телефонные сети. Поэтому приведённые здесь сведения о Dial-up-модемах носят познавательный характер, необходимый для понимания дальнейшего материала.

С одной стороны, технологически модем – это одно из старых и заслуженных устройств передачи данных, это вершина радиотех-

ники: сложные аналоговые узлы сопрягаются с цифровыми схемами обработки данных, используя последние достижения теории.

С другой стороны, трудно придумать более странный и бестолковый прибор: сначала, используя сложную схему модуляции, данные упаковываются в трёхкилоге́рцевую полосу пропускания аналогового телефонного канала, но на первом же концентраторе АТС происходит второе преобразование – канал оцифровывается и в дальнейшем данные передаются в дважды преобразованном виде. На последнем концентраторе перед «последней милей» пользователя данные снова преобразуются в аналоговый сигнал, чтобы попасть на модем пользователя, который совершит аналоговую демодуляцию. Наконец, данные переданы, а модемы и телефонное оборудование совершили кучу лишней работы.

1.8.3 Коммутируемый доступ через сеть ISDN

Целью создания технологии ISDN (Integrated Services Digital Network – цифровая сеть с интегрированным обслуживанием) было построение всемирной сети, которая должна была бы прийти на смену телефонной сети и, будучи такой же доступной и распространённой, предоставлять миллионам своих пользователей разнообразные услуги, как телефонные, так и передачи данных. Передача телевизионных программ по ISDN не предполагалась, поэтому было решено ограничиться пропускной способностью абонентского окончания для массовых пользователей в 128 кбит/с.

Если бы цель разработчиков ISDN была достигнута в полной мере, то проблема доступа домашних пользователей к Интернету и корпоративным сетям была бы окончательно решена. Однако по многим причинам внедрение ISDN происходило очень медленно – процесс, который начался в 80-е годы прошлого века, растянулся больше чем на десять лет, так что к моменту выхода на рынок некоторые услуги сети ISDN морально устарели. Скорость доступа 128 кбит/с сегодня для пользователей уже далеко недостаточна.

Сеть ISDN не стала той новой публичной сетью, на роль которой она претендовала, хотя её услуги, перечисленные ниже, достаточно интересны.

- некоммутируемые средства (выделенные цифровые каналы);
- коммутируемая телефонная сеть общего пользования;
- сеть передачи данных с коммутацией каналов;
- сеть передачи данных с коммутацией пакетов;
- сеть передачи данных с трансляцией кадров (режим сети Frame Relay);

– средства контроля и управления работой сети.

Из вышеперечисленных услуг разберём вкратце использование ISDN для передачи данных. Несмотря на значительные отличия от аналоговых телефонных сетей, сети ISDN используются в основном так же, как аналоговые, то есть как сети с коммутацией каналов, но только более скоростные, поскольку качество цифровых каналов выше, чем аналоговых: процент искажённых кадров оказывается ниже, а полезная скорость обмена данными выше.

В зависимости от интерфейса, используемого сетью ISDN, в качестве конечного терминального оборудования в одном случае может быть компьютер и даже маршрутизатор, в другом случае – цифровой телефон. Для подключения компьютерного оборудования к сети ISDN необходимо использовать терминальный адаптер, который согласует интерфейс компьютера с интерфейсом сети ISDN. Для компьютеров терминальные адаптеры выпускаются в формате сетевых адаптеров.

Таким образом, для удалённого доступа через сеть ISDN необходимо оснастить компьютеры пользователей терминальными адаптерами ISDN, а у поставщика услуг установить маршрутизатор, имеющий интерфейс сети ISDN. В этом случае максимальная скорость доступа для отдельного пользователя будет равна 128 кбит/с. Как видим, она не сильно превышает скорость Dial-up-модема (56 кбит/с), использующего протокол V.90.

К сожалению, цены на адаптеры ISDN и тарифная политика телефонных компаний несообразны с пропускной способностью, предоставляемой этой службой. Напротив, акустические Dial-up-модемы выпускались нетелефонными компаниями при сильной конкуренции, что привело к падению цен на них до технологически обусловленного минимума.

Низкая цена приобретения и эксплуатации Dial-up-модемов привела к их массовому распространению. Эти модемы обеспечивали почти всё, что заложено в спецификациях ISDN. Массовое распространение таких модемов привело к тому, что в любой операционной системе они поддерживались соответствующими драйверами. Адаптеры же ISDN всегда требовали докачки и обновлений драйверов и сложной настройки. В результате полная стоимость владения адаптером ISDN оказалась очень высокой и даже при более высокой пропускной способности данных они были полностью неконкурентоспособными.

Тарифная политика телефонистов не отличалась разумностью – по приблизительным оценкам количество абонентов сети ISDN в раз-

витых странах составляет в среднем 5 % от общего количества абонентов аналоговой телефонии.

1.8.4 Доступ по технологии xDSL

На смену цифровому окончанию ISDN пришло семейство технологий под общим названием xDSL, которое включает в себя:

- асимметричное цифровое абонентское окончание – ADSL (Asymmetric Digital Subscriber Line), которое часто называют широкополосным доступом;
- симметричное цифровое абонентское окончание – SDSL (Symmetric Digital Subscriber Line);
- сверхбыстрое цифровое абонентское окончание – VDSL (Very high-speed Digital Subscriber Line).

Эти цифровые окончания были разработаны для обеспечения скоростного доступа в Интернет массовых индивидуальных пользователей, квартиры которых оснащены обычными абонентскими телефонными окончаниями. Появление технологии ADSL можно считать революционным событием для массовых пользователей Интернета, потому что для них оно означало повышение скорости доступа в десятки раз (а то и более) без какого бы то ни было изменения кабельной проводки в квартире и доме.

Для доступа через ADSL, так же как и для аналогового коммутируемого доступа, нужны телефонные абонентские окончания и модемы. Однако принципиальным отличием доступа через ADSL от коммутируемого является то, что ADSL-модемы работают только в пределах абонентского окончания, в то время как коммутируемые модемы используют возможности телефонной сети, устанавливая в ней соединение «из конца в конец» , которое проходит через несколько транзитных коммутаторов.

Традиционные телефонные модемы (например V.34, V.90) должны обеспечивать передачу данных на канале с полосой пропускания в 3100 Гц, ADSL-модемы получают в своё распоряжение полосу порядка 1 МГц – эта величина зависит от длины и полосы пропускания кабеля, проложенного между помещением пользователя и точкой доступа.

Схема доступа через ADSL показана на рисунке 3. Схема ADSL позволяет получить одновременный доступ для телефонных разговоров и передачи компьютерных данных.

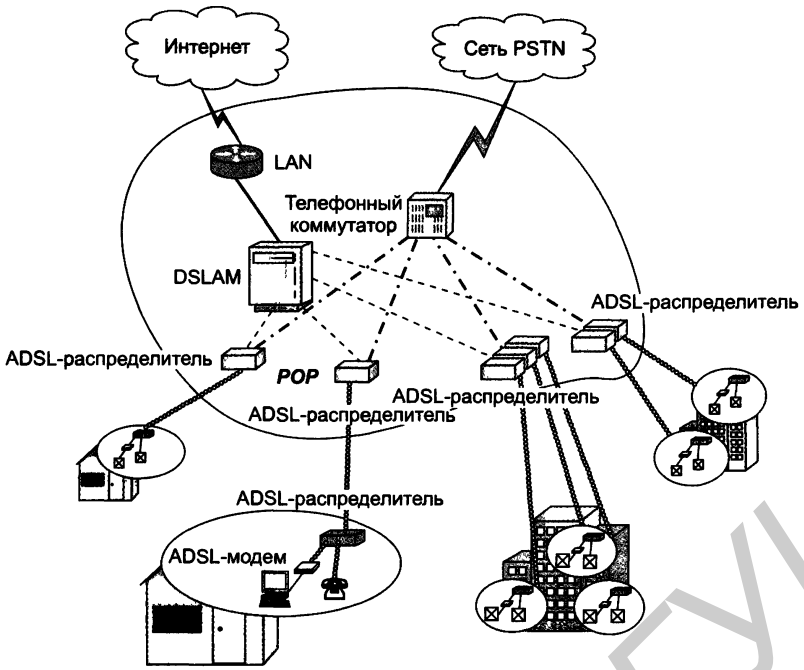


Рисунок 3 – Схема работы ADSL-модема

ADSL-модемы, подключённые между абонентом и точкой доступа провайдера, используют полосу частот от 20 кГц до 1 МГц. В этой полосе 150 кГц отводится восходящему каналу (upload), а остальное – около 800 кГц – высокоскоростному нисходящему каналу передачи данных из сети в компьютер (download). Полоса частот в 4 кГц для обычных телефонных разговоров отсекается полосовым фильтром и в ADSL-модем не попадает, вот почему возможна одновременная работа телефона и ADSL-модема.

Из таблицы 1 тарифных планов Белтелекома по состоянию на июль 2015 года мы видим, как разделяется и тарифицируется трафик по восходящему каналу upload и по нисходящему – download, видно также, что эти скорости не равны. В данном случае

download > upload .

Это и означает «асимметричность» ADSL-модема.

Таблица 1 – Тарифные планы Белтелекома

Тарифы для физических лиц	Стоимость
Домосед Классик (скорость приём/передача до **2048**/**512** кбит/с)	105 000
Домосед плюс (скорость приём/передача до **3072**/**512** кбит/с)	116 100
Домосед XXL (скорость приём/передача до **4096**/**512** кбит/с)	145 200
СуперДомосед (скорость приём/передача до **6144**/**512** кбит/с)	198 000
Социальный анлим (скорость приём/передача до **1024**/**512** кбит/с)	42 300
Социальный анлим 2 (скорость приём/передача до **2048**/**512** кбит/с)	45 000
Домосед Ультра (скорость приём/передача до **8192**/**512** кбит/с)	216 000

Поступив к провайдеру, модулированные сигналы преобразуются в дискретную форму и отправляются на IP-маршрутизатор. Далее данные попадают в компьютерную сеть поставщика услуг и доставляются в соответствии с IP-адресами назначения на конечный пункт. Если абонент у себя разговаривает по телефону, то голосовые сигналы поступают к провайдеру вместе с компьютерными, но полосовой фильтр вычленяет полосу 4 кГц, и она передаётся на телефонный коммутатор, который обрабатывает их обычным образом.

Работа ADSL-модемов регламентируется стандартами, приведёнными в таблице 2.

Таблица 2 – Стандарты ADSL-соединения

Стандарт	Год
ITU-T G.991.2 (скорость приём/передача до **12**/**1.3** Мбит/с)	1999
ITU-T G.991.5 (ADSL2+) (скорость приём/передача до **24**/**1.3** Мбит/с)	2003
ITU-T G.992.3 VDSL2 (Very high-speed DSL2) (скорость приём/передача до **250**/**5.2** Мбит/с)	2006

Эти высокоскоростные стандарты, приведённые в таблице 2, рассчитаны на высококачественные телефонные линии, если качество проводки низкое, а расстояние до АТС значительное; на повышение скорости при применении модема нового стандарта рассчитывать не приходится.

Метод SDSL – симметричное цифровое абонентское окончание, позволяющее на одной паре абонентского окончания организовать два симметричных канала передачи данных. Канал тональной частоты в этом случае не предусматривается. Скорости каналов в восходящем и нисходящем направлениях выравнены и составляют по 2 Мбит/с.

Метод SDSL разработан для небольших офисов, локальные сети которых содержат собственные источники информации, web-серверы или серверы баз данных. Трафик такой сети будет скорее всего симметричный, так как доступ через SDSL потребуется не только к внешним сетям из локальных сетей, но и к таким источникам информации извне. В технологии SDSL используется вся полоса частот, в том числе и телефонная полоса 4 кГц, поэтому при работе SDSL-модема по телефону поговорить не удастся.

Широкое применение доступа через xDSL наносит еще один удар технологии ISDN. При применении этого типа абонентских окончаний пользователь получает ещё и интегрированное обслуживание двух сетей: телефонной и компьютерной. Но для пользователя наличие двух сетей оказывается незаметным, для него только ясно, что он может одновременно пользоваться обычным телефоном и подключённым к Интернету компьютером. Скорость же компьютерного доступа при этом превосходит возможности интерфейса PRI сети ISDN при существенно более низкой стоимости, определяемой низкой стоимостью инфраструктуры IP-сетей.

1.8.5 Доступ по технологии xPON

GPON (Gigabit-capable Passive Optical Networks) – наиболее быстро развивающаяся и перспективная технология широкополосного мультисервисного доступа по оптическому волокну.

К пользователю приходит уже не медный кабель, а волоконно-оптический. При этом ему предоставляется весь ресурс оптического кабеля, который заводится непосредственно в квартиру, в отличие от операторов домовых сетей, где канал выделяется на дом и делится в равной степени между подключёнными жильцами. Такой сервис открывает множество возможностей:

- асимметричное цифровое абонентское окончание – ADSL, которое часто называют широкополосным доступом;
- доступ в Интернет на высокой скорости от 100 Мбит/с до1 Гбит/с и выше в направлении от сети к пользователю (download);

– мультисервисный доступ, при котором абоненту может быть предоставлен комплекс базовых услуг: телефонная связь; домофон; доступ к сети Интернет; интерактивное телевидение, к которому можно одновременно подключить сразу несколько ТВ-приёмников в квартире или офисе, обеспечить трансляцию программ как в высоком разрешении HD, так и в 4K; охранная сигнализация, а в дальнейшем – установка системы «умный дом».

Технология xPON предоставляет стабильное качество услуг и не так уязвима, как xDSL, так как качество услуг на PON не зависит от таких параметров, как длина абонентской линии, сечение жилы, «сезонное» сопротивление изоляции. Если же сравнивать xPON с технологией Ethernet, то преимуществом первой является то, что она не требует использования активного оборудования на местах. Основное оборудование находится на площадях оператора, а значит, лучше защищено и работает стабильно, меньше точек отказа оборудования.

Для подключения пользователя по технологии xPON необходимо установить модем – ONT (Optical Network Terminal), после чего возможно подключение всех услуг.

Пассивная* оптическая сеть доступа PON (Passive Optical Networks) основана на древовидной волоконно-кабельной архитектуре с пассивными оптическими разветвителями на узлах, представляет экономичный способ обеспечить широкополосную передачу информации. При этом архитектура PON обладает необходимой эффективностью наращивания узлов сети и пропускной способности в зависимости от настоящих и будущих потребностей абонентов.

Развитие сетей доступа PON происходило следующим образом.

1. Октябрь 1998 года: появляется первый стандарт ITU-T G.983.1, базирующийся на транспорте ячеек ATM (Asynchronous Transfer Mode) в дереве PON и получивший название APON (ATM PON).

2. Март 2001 года: появляется рекомендация G.983.3, закрепляющая понятие BPON (broadband PON) и добавляющая новые функции в стандарт PON:

– передача разнообразных приложений (голос, видео, данные), что фактически позволило производителям добавлять соответствующие интерфейсы на OLT (Optical Line Terminal) для подключения к магистральной сети и на або-

* «Пассивная» в аббревиатуре PON обозначает отсутствие активных, то есть энергопотребляющих компонентов.

нентские узлы ONT (Optical Network Terminal) для подключения абонентов;

– расширение спектрального диапазона открывает возможность для дополнительных услуг на других длинах волн в условиях одного и того же дерева PON, например широковещательное телевидение на третьей длине волны (triple play).

3. Ноябрь 2000 года: комитет LMSC (LAN/MAN standards committee) IEEE создаёт специальную комиссию под названием «Ethernet первая миля» EFM (Ethernet in the first mile) 802.3ah, реализовав тем самым пожелания многих экспертов построить архитектуру сети PON, наиболее приближённую к широко распространённым в настоящее время сетям Ethernet.

4. Октябрь 2003 года: принят Стандарт GPON ITU-T Rec. G.984.3 GPON. GPON предоставляет масштабируемую структуру кадров при скоростях передачи от 622 Мбит/с до 2,5 Гбит/с и допускает системы как с одинаковой скоростью передачи прямого и обратного потока в дереве PON, так и с разной. GPON базируется на стандарте ITU-T G.704.1 GFP (Generic Framing Protocol – общий протокол кадров), обеспечивая инкапсуляцию в синхронный транспортный протокол любого типа сервиса, в том числе TDM. Исследования показывают, что даже в самом худшем случае распределения трафика и колебаний потоков утилизация полосы составляет 93 % по сравнению с 71 % в APON, не говоря уже о EPON. Технические характеристики различных технологий xPON сведены в таблице 3.

Таблица 3 – Сравнительный анализ технологий APON, EPON и GPON

Характеристики	APON (BPON)	EPON	GPON
Институты стандартизации / альянсы	ITU-T SG15 / FSAN	IEEE / EFMA	ITU-T SG15 / FSAN
Дата принятия стандарта	октябрь 1998	июль 2004	октябрь 2003
Стандарт	ITU-T G.981.x	IEEE 802.3ah	ITU-T G.984.x
Скорость передачи, прямой/обратный поток, Мбит/с	155/155 622/155 622/622	1000/1000	1244/155, 622,1244 2488/622,1244, 2488
Базовый протокол	ATM	Ethernet	SDH
Линейный код	NRZ	8B/10B	NRZ
Максимальный радиус сети, км	20	20 (>30[1])	20
Максимальное число абонентских узлов на одно волокно	32	16	64 (128)
Приложения	Любые	IP, данные	Любые

Характеристики	APON (BPON)	EPON	GPON
Коррекция ошибок FEC	Предусмотрена	Нет	Необходима
Длины волн прямого/ обратного потоков, нм	1550/1310 (1480/1310)	1550/1310 (1310/1310)	1550/1310 (1480/1310)
Динамическое распределение полосы	Есть	Поддержка	Есть
IP-фрагментация	Есть	Нет	Есть
Защита данных	Шифрование открытыми ключами	Нет	Шифрование открытыми ключами
Резервирование	Есть	Нет	Есть
Оценка поддержки голосовых приложений и QoS	Нет	Нет	Нет

В последнее время в Республике Беларусь Национальный оператор электросвязи Белтелеком осуществляет плановое подключение граждан к услуге xPON. В силу технической сложности этого метода Белтелеком предлагает сначала вам протестировать техническую возможность вашего абонентского окончания для подключения по xPON со своей web-странички: http://www.byfly.by/gPON-spisok-domov. Эта простая процедура требует от абонента ввести в поля web-странички свои адресные реквизиты: регион, город, улица и номер дома.

В результате тестирования вы сможете узнать, подключён ваш дом к этой передовой оптоволоконной технологии или нет. К сожалению, охватить всех граждан пока не представляется возможным. В число счастливчиков в первую очередь попали жители мегаполисов. На рисунке 4 изображена карта районов охвата этой услугой города Минска.

В таблице 4 представлены тарифные планы по услуге GPON, называемые «Тарифные планы высокоскоростного нелимитируемого доступа в сеть Интернет». Данные в этой таблице приведены по состоянию на июль 2015 года.

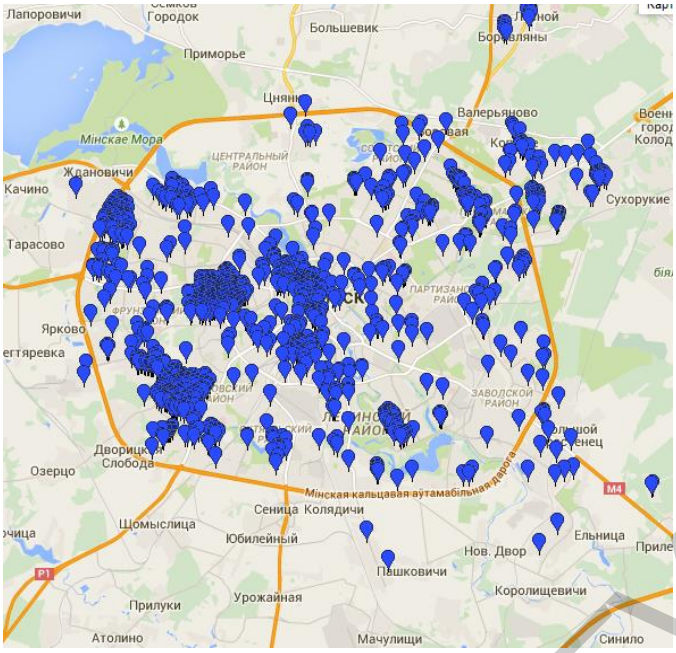


Рисунок 4 – Карта охвата услуги xPON в городе Минске

Обратите внимание, что подключение абонентского окончания по технологии xPON тоже асимметрично, то есть как и для технологии ADSL

download > upload .

Таблица 4 – Тарифные планы Белтелекома для GPON

Тарифы для физических лиц	Стоимость
Рекорд 5 (скорость приём/передача до 5/2.5 Мбит/с)	125 000
Рекорд 10 (скорость приём/передача до 10/5 Мбит/с)	150 000
Рекорд 15 (скорость приём/передача до 15/7.5 Мбит/с)	175 000
Рекорд 20 (скорость приём/передача до 20/10 Мбит/с)	200 000
Рекорд 50 (скорость приём/передача до 50/25 Мбит/с)	330 000
Рекорд 100 (скорость приём/передача до 100/50 Мбит/с)	390 000

2 Практическая часть

2.1 Лабораторная работа. Стандартные команды консоли для настройки и работы с компьютерной сетью

В компьютерных сетях в качестве рабочих станций и серверов могут быть подключены компьютеры с различными операционными системами: Linux, Mac OS, Windows, различные мэйнфрэймы; а также подключается специальное сетевое оборудование со специальными операционными системами, например коммутаторы, маршрутизаторы. С другой стороны, компьютерная сеть едина и для своего управления не делает различия между разными операционными системами.

Упражнение для самостоятельной работы 1. *В таблице 5 приведён перечень практически всех консольных команд, используемых в ОС Linux и Windows для работы и настройки сети. Выберите свой вариант с пятью командами из таблицы 6 и выполните следующее задание.*

Дайте для каждой выбранной вами команды развёрнутое описание и приведите основные ключи. Выясните, может ли описываемая команда работать в пакетном режиме (batch mode) интерактивном режиме или только в режиме командной строки?

Если для описываемой команды возможен интерактивный режим, то расскажите; как в него войти, а самое главное – как из него выйти ничего не испортив. Если для описываемой команды возможен пакетный режим, то объясните, каков простейший синтаксис и правила написания такого файла, из которого команда может считывать команды, ключи и данные.

Для выполнения задания запустите на вашем компьтере консоли Windows и Linux. Воспользуйтесь обеими консолями для выполнения задания.

Таблица 5 – Команды консоли для работы с сетью

№	Команда OS Linux	Команда OS Windows	Описание действия и применение команды
1	**arp**	**arp**	Выводит таблицу соответствия ARP
2	**dhclient**	**–**	DHCP-клиент для конфигурирования компьютеров и раздачи IP-адресов

№	Команда OS Linux	Команда OS Windows	Описание действия и применение команды
3	**dig**	**–**	Утилита настройки и поиска для DNS-администраторов
4	**ethtool**	**–**	Утилита для настройки сетевого адаптера и оборудования в Linux
5	**fsck**	**–**	Утилита для тестирования и мелкого ремонта для большинства файловых систем Linux
6	**ftp**	**ftp**	Обмен файлами с компьютером, на котором запущена служба сервера FTP
7		**getmac**	Позволяет отобразить MAC-адреса сетевых адаптеров компьютера
8	**host**	**–**	Утилита поиска IP-адреса по доменному имени
9	**hostname**	**hostname**	Выводит имя текущего хоста
10	**ifconfig**	**ipconfig**	Общая информация о сетевой конфигурации
11	**ifplugd**	**–**	Домен обнаружения связи сетевого интерфейса устройств Ethernet
12	**ifup**	**–**	Для предварительной настройки интерфейса
13	**ifdown**	**–**	Для высвобождения адреса и закрытия интерфейсов
14	**ifstatus**	**–**	Проверка конфигурации маршрутов интерфейса
15	**ifrenew**	**–**	Используется для обновления аренды DHCP требуемого интерфейса
16	**ifprobe**	**–**	Проверка файлов конфигурации
17	**iwconfig**	**–**	Конфигурация сети Wi-Fi
18	**mtr**	**–**	Утилита сетевой диагностики, скомпилированная без GTK. Для работы с GTK используется **xmtr**
19	**net***	**net**	Многофункциональная команда для сетевых параметров и конфигурации компьютера
20	**netstat**	**netstat**	Отображение статистики протокола и текущих сетевых подключений TCP/IP
21	**nmap**	**–**	Утилита для исследования сети и сканирования портов
22		**netsh**	Многофункциональная команда сетевых параметров и конфигурации

* Команда работает, если установлен пакет Samba.

№	Команда OS Linux	Команда OS Windows	Описание действия и применение команды
23	**nslookup**	**nslookup**	Интерактивная команда: вывод сведений об узле или домене с помощью сервера по умолчанию
24	**ping**	**ping**	Контроль доступности порта с определённым IP-адресом
25		**pathping**	Контроль доступности маршрута определённого IP-адреса по списку узлов
26	**route**	**route**	Обработка таблиц сетевых маршрутов с использованием масок и метрик
27		**sfc**	Проверка целостности ресурсов всех защищённых системных файлов
28	**telnet**	**telnet**	Команда, активирующая протокол работы с удалённым терминалом
29	**traceroute**	**tracert**	Выводит маршрут со списком узлов до определённого IP-адреса
30	**scp**	**–**	Программа копирования удалённых файлов между хостами в сети
31	**sftp**	**–**	Интерактивная команда передачи зашифрованных файлов
32	**ssh**	**–**	SSH-клиент – это программа для безопасного входа на удалённый компьютер

Таблица 6 – Варианты выполнения задания

Номер варианта	Команды	
	OS Linux	OS Windows
1	arp, ifdown, telnet	ftp, nslookup
2	dhclient, ifstatus, net	getmac, tracert
3	fsck, ifrenew, ssh	arp, route
4	ftp, ifprobe, scp	hostname, pathping
5	host, iwconfig, traceroute	ipconfig, sfc
6	hostname, mtr, nmap, sftp	net, ping
7	ifup, netstat, route, ethtool	netsh
8	ifconfig, nslookup, ping	netstat, telnet

Замечание. Иногда при попытке запуска команды в консоли Linux, например

duralei@strekoza:/usr/share> ifconfig ,

операционная система может выдать сообщение

Absolute path to 'ifconfig' is '/sbin/ifconfig', so running it may require superuser privileges (eg. root)*,

тогда попробуйте для выполнения этой команды набрать полный путь*:

duralei@strekoza:/usr/share> /sbin/ifconfig.

* Полный путь к «ifconfig» – это «/sbin/ifconfig», и для её выполнения могут потребоваться привилегии суперпользователя (например root).

2.2 Лабораторная работа. Стандартные стеки коммуникационных протоколов

Важнейшим направлением стандартизации в области вычислительных сетей является стандартизация коммуникационных протоколов. Наиболее известными стеками протоколов являются OSI, TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA (не все из них применяются сегодня на практике).

2.2.1 Стек OSI

Важно различать модель OSI и стек протоколов OSI. В то время как модель OSI является концептуальной схемой взаимодействия открытых систем, стек OSI (рисунок 5) представляет собой набор спецификаций конкретных протоколов [5].

Рисунок 5 – Стек протоколов OSI

В отличие от других стеков протоколов, стек OSI полностью соответствует модели OSI, включая спецификации протоколов для всех семи уровней взаимодействия, определённых в этой модели. Это и понятно, разработчики стека OSI использовали модель OSI как прямое руководство к действию.

Протоколы стека OSI отличает сложность и неоднозначность спецификаций. Эти свойства явились результатом общей политики разработчиков стека, стремившихся учесть в своих протоколах всё многообразие уже существующих и появляющихся технологий.

На физическом и канальном уровнях стек OSI поддерживает протоколы Ethernet, Token Ring, FDDI, а также протоколы LLC, X.25 и ISDN, то есть использует все разработанные вне стека популярные протоколы нижних уровней, как и большинство других стеков.

Сетевой уровень включает сравнительно редко используемые протоколы Connectionoriented Network Protocol (CONP) и Connectionless Network Protocol (CLNP). Как следует из названий, первый из них ориентирован на соединение (connection-oriented), второй – нет (connectionless).

Более популярны протоколы маршрутизации стека OSI: ES-IS (End System – Intermediate System) между конечной и промежуточной системами и IS-IS (Intermediate System – Intermediate System) между промежуточными системами.

Транспортный уровень стека OSI в соответствии с функциями, определёнными для него в модели OSI, скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают требуемое качество обслуживания независимо от нижележащего сетевого уровня. Чтобы обеспечить это, транспортный уровень требует, чтобы пользователь задал нужное качество обслуживания.

Службы прикладного уровня обеспечивают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее популярными являются служба каталогов (стандарт X.500), электронная почта (X.400), протокол виртуального терминала (VTP), протокол передачи, доступа и управления файлами (FTAM), протокол пересылки и управления работами (JTM).

2.2.2 Стек IPX/SPX

Стек IPX/SPX является оригинальным стеком протоколов фирмы Novell, разработанным для сетевой операционной системы NetWare еще в начале 80-х годов прошлого века. Структуру стека IPX/SPX и его соответствие модели OSI иллюстрирует рисунок 6. Название стеку дали протоколы сетевого и транспортного уровней – Internetwork Packet Exchange (IPX) и Sequenced Packet Exchange (SPX). К сетевому уровню этого стека отнесены также протоколы маршрутизации RIP и NLSP. А в качестве представителей трёх верхних уровней на рисунке приведены два популярных протокола: протокол удалённого доступа к файлам NetWare Core Protocol (NCP) и протокол объявления о сервисах Service Advertising Protocol (SAP).

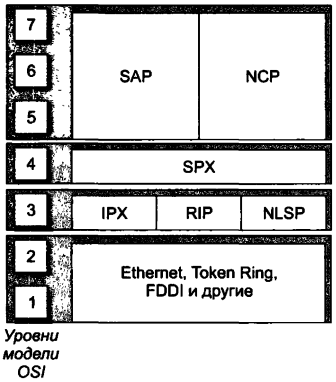


Рисунок 6 – Стек протоколов IPX/SPX

Многие особенности стека IPX/SPX обусловлены ориентацией ранних версий ОС NetWare на работу в локальных сетях небольших размеров, состоящих из персональных компьютеров со скромными ресурсами. Понятно, что для таких компьютеров компании Novell нужны были протоколы, на реализацию которых требовалось бы минимальное количество оперативной памяти (ограниченной в IBM-совместимых компьютерах под управлением MS-DOS объемом 640 Кбайт) и которые быстро работали бы на процессорах небольшой вычислительной мощности. В результате протоколы стека IPX/SPX до недавнего времени отлично справлялись с работой в локальных сетях. Однако в крупных корпоративных сетях они слишком перегружали медленные глобальные связи широковещательными пакетами, интенсивно использующимися несколькими протоколами этого стека, например протоколом SAP. Это обстоятельство, а также тот факт, что стек IPX/SPX является собственностью фирмы Novell и на его реализацию нужно получать лицензию (то есть открытые спецификации не поддерживались), долгое время ограничивали распространённость его только сетями NetWare.

2.2.3 Стек NetBIOS/SMB

Стек NetBIOS/SMB является совместной разработкой компаний IBM и Microsoft (рисунок 7). На физическом и канальном уровнях этого стека также задействованы уже получившие распространение протоколы, такие как Ethernet, Token Ring, FDDI, а на верхних уровнях – специфические протоколы NetBEUI и SMB.

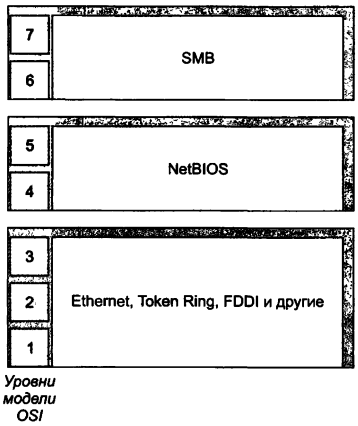


Рисунок 7 – Стек NetBiOS/SMB

Протокол Network Basic Input/Output System (NetBIOS) появился в 1984 году как сетевое расширение стандартных функций базовой системы ввода-вывода (BIOS) IBM PC для сетевой программы PC Network фирмы IBM. В дальнейшем этот протокол был заменён так называемым протоколом расширенного пользовательского интерфейса NetBEUI (NetBIOS Extended User Interface). Для совместимости приложений в качестве интерфейса к протоколу NetBEUI был сохранён интерфейс NetBIOS. NetBEUI разрабатывался как эффективный протокол, потребляющий немного ресурсов и предназначенный для сетей, насчитывающих не более 200 рабочих станций. Этот протокол содержит много полезных сетевых функций, которые можно отнести к транспортному и сеансовому уровням модели OSI, однако с его помощью невозможна маршрутизация пакетов. Это ограничивает применение протокола NetBEUI локальными сетями, не разделёнными на подсети, и делает невозможным его использование в составных сетях.

Протокол Server Message Block (SMB) поддерживает функции сеансового уровня, уровня представления и прикладного уровня. На основе SMB реализуется файловая служба, а также службы печати и передачи сообщений между приложениями.

2.2.4 Стек TCP/IP

Стек TCP/IP был разработан по инициативе Министерства обороны США более 20 лет назад для связи экспериментальной сети ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Большой вклад в развитие стека TCP/IP, который получил свое название по популярным протоколам IP и TCP, внёс университет Беркли, реализовав протоколы стека в своей версии ОС Unix. Популярность этой операционной системы привела к широкому распространению протоколов TCP,

IP и других протоколов стека. Сегодня этот стек используется для связи компьютеров в Интернете, а также в огромном числе корпоративных сетей.

2.2.5 Соответствие популярных стеков протоколов модели OSI

На рисунке 8 показано, в какой степени популярные стеки протоколов соответствуют рекомендациям модели OSI. Как мы видим, часто это соответствие весьма условно. В большинстве случаев разработчики стеков отдавали предпочтение скорости работы сети в ущерб модульности – ни один стек, кроме стека OSI, не разбит на семь уровней. Чаще всего в стеке явно выделяются 3-4 уровня: уровень сетевых адаптеров, в котором реализуются протоколы физического и канального уровней, сетевой уровень, транспортный уровень и уровень служб, вбирающий в себя функции сеансового уровня, уровня представления и прикладного уровня.

Структура стеков протоколов часто не соответствует рекомендуемому моделью OSI разбиению на уровни и по другим причинам. Чем характеризуется идеальное многоуровневое построенние? С одной стороны, необходимо соблюсти принцип иерархии: каждый вышележащий уровень обращается с запросами только к нижележащему, а нижележащий предоставляет свои сервисы только непосредственно соседствующему с ним вышележащему. В стеках протоколов это приводит к тому, что PDU вышележащего уровня всегда инкапсулируется в PDU нижележащего.

С другой же стороны, идеальная многоуровневая декомпозиция предполагает, что все модули, отнесенные к одному уровню, ответственны за решение общей для всех них задачи. Однако эти требования часто вступают в противоречие. Например, основной функцией протоколов сетевого уровня стека TCP/IP (так же как и сетевого уровня OSI) является передача пакетов через составную сеть. Для решения этой задачи в стеке TCP/IP предусмотрено несколько протоколов: продвижения IP-пакетов и маршрутизации RIP, OSPF. Если считать признаком принадлежности к одному и тому же уровню общность решаемых задач, то, очевидно, протокол IP и протоколы маршрутизации должны быть отнесены к одному уровню. Вместе с тем, если принять во внимание, что сообщения протокола RIP инкапсулируются в UDP-дейтаграммы, а сообщения протокола OSPF – в IP-пакеты, то, следуя формально принципу иерархической организации стека, OSPF следовало бы отнести к транспортному, а RIP – к прикладному уровню. На практике же протоколы маршрутизации обычно включают в сетевой уровень.

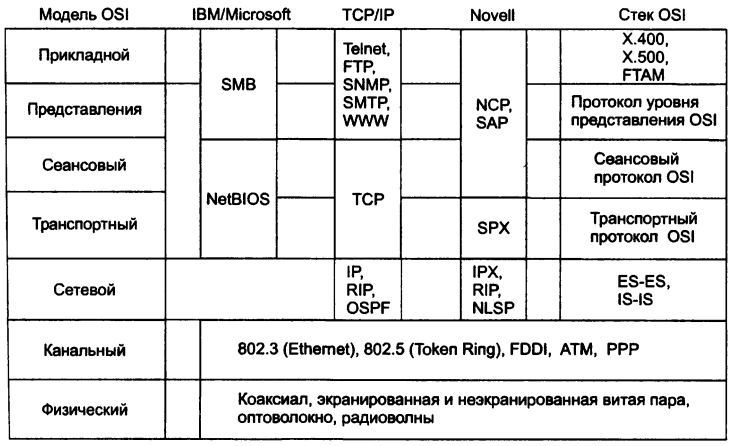


Рисунок 8 – Соответствие распространённых стеков протоколов модели OSI

2.2.6 Практические задания

Упражнение для самостоятельной работы 2. *Можно ли представить вариант модели взаимодействия открытых систем с другим количеством уровней, например 8 или 5?*

Упражнение для самостоятельной работы 3. *На каком уровне модели OSI работают прикладные программы?*

Упражнение для самостоятельной работы 4. *На каком уровне модели OSI работают сетевые службы?*

Упражнение для самостоятельной работы 5. *На двух компьютерах установлено идентичное программное и аппаратное обеспечение, за исключением того что драйверы сетевых адаптеров Ethernet поддерживают разные интерфейсы с протоколом сетевого уровня IP. Будут ли эти компьютеры нормально взаимодействовать, если их соединить в сеть?*

Упражнение для самостоятельной работы 6. *С помощью многоуровневых моделей, представленных на рисунке 9, опишите процесс заказа и доставки пиццы, указав взаимодействие всех уровней.*

а – трёхуровневая модель передачии сообщения по телефону;
б **–** трёхуровневая модель доставки товара по автостраде

Рисунок 9 – Иллюстрация трёхуровневой композиции (горизонтальные стрелки – связь по протоколам, вертикальные – по интерфейсам)

Упражнение для самостоятельной работы 7. *Перечислите основные недостатки многоуровневого подхода к протоколам.*

Упражнение для самостоятельной работы 8. *В таблице 7 приведены протоколы, обеспечивающие сетевое взаимодействие различного оборудования. Выберите один из 21 варианта и кратко охарактеризуйте каждый из девяти протоколов своего варианта, заполнив три пустых поля таблицы, где*:

– кратко опишите протокол;
– поставьте описываемый протокол в соответствие определённому уровню модели OSI;
– определите первоначальное происхождение протокола.

Таблица 7 – Сетевые протоколы. Варианты выполнения задания

№	Протокол	Соответствие уровню OSI	Первоначальное происхождение	Краткое описание
1	2	3	4	5
	Вариант 1			
1	Ethernet,			
2	IEEE 802.11			
3	ATM, Asynchronous Transfer Mode			
4	Open Systems Interconnection (OSI) Model			
5	PIM-SM, Protocol Independent Multicast Sparse Mode			
6	DNS, Domain Name System			
7	OSCAR, AOL Instant Messenger Protocol			
8	PNRP, Peer Name Resolution Protocol			
9	SSL, Secure Sockets Layer			
	Вариант 2			
1	IEEE 802.15 (Bluetooth)			
2	ARCnet			
3	IPv4/IPv6, Internet Protocol			
4	PIM-DM, Protocol Independent Multicast Dense Mode			
5	SOCKS, SOCKet Secure			
6	RARP, Reverse Address Resolution Protocol			
7	Rlogin, Remote Login in UNIX Systems			
8	RPC, Remote Procedure Call			
9	ES-IS End System – Intermediate System			
	Вариант 3			
1	IrDA Infrared Data Association			
2	CAN Controller Area Network,			
3	DVMRP, Distance Vector Multicast Routing Protocol			
4	IPsec, Internet Protocol Security			
5	ZIP, Zone Information Protocol			
6	SNMP, Simple Network Management Protocol			
7	RELP, Reliable Event Logging Protocol			
8	RIP, Routing Information Protocol			
9	TLS Transport Layer Security			
	Вариант 4			
1	EIA-485 Electronics Industries Alliance			
2	Econet,			
3	ARP, Address Resolution Protocol			
4	IPX, Internetwork Packet Exchange			
5	SDP, Sockets Direct Protocol			
6	BitTorrent			
7	RDP, Remote Desktop Protocol			
8	RTMP, Real Time Messaging Protocol			
9	xDSL digital subscriber line			

1	2	3	4	5
Вариант 5				
1	RS-232, Recommended Standard 232			
2	Ethernet			
3	ICMP, Internet Control Message Protocol			
4	RIP, Routing Information Protocol			
5	AFP, Apple Filing Protocol			
6	BOOTP, bootstrap protocol			
7	SDP, Session Description Protocol			
8	SIP, Session Initiation Protocol			
Вариант 6				
1	EIA-422, Electronics Industries Alliance			
2	EAPS, Ethernet Automatic Protection Switching			
3	IGMP, Internet Group Management Protocol			
4	DDP, Datagram Delivery Protocol			
5	ICA, Independent Computing Architecture, the Citrix system core protocol			
6	Freenet			
7	NTP, Network Time Protocol			
8	RTP, Real-time Transport Protocol			
Вариант 7				
1	EIA-423			
2	Fiber Distributed Data Interface (FDDI),			
3	PIM-SM, Protocol Independent Multicast Sparse Mode			
4	BGP, Border Gateway Protocol			
5	LPP, Lightweight Presentation Protocol			
6	CMIP, Common Management Information Protocol			
7	DeviceNet			
8	SAP, Session Announcement Protocol			
9	X.500, Directory Access Protocol (DAP)			
Вариант 8				
1	RS-449, Recommended Standard 449			
2	Frame Relay,			
3	PIM-DM, Protocol Independent Multicast Dense Mode			
4	ADSP, Протокол потоков данных AppleTalk (AppleTalk Data Stream Protocol)			
5	NCP, NetWare Core Protocol			
6	eDonkey			
7	RTPS, Real Time Publish Subscribe			
8	RTSP, Real Time Streaming Protocol			
Вариант 9				
1	RS-485, Recommended Standard 485			
2	HDLC, High-Level Data Link Control			
3	IPsec, Internet Protocol Security			
4	ASP, Сеансовый протокол AppleTalk (AppleTalk Session Protocol)			
5	NDR, Network Data Representation			
6	SLP, Service Location Protocol			

1	2	3	4	5
7	SMB, Server Message Block			
8	SNTP, Simple Network Time Protocol			
Вариант 10				
1	ADSL, asymmetric + DSL			
2	IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers),			
3	IPX, Internetwork Packet Exchange			
4	H.245, Call Control Protocol for Multimedia Communication			
5	Telnet (a remote terminal access protocol)			
6	SSH, Secure Shell			
7	SSMS, Secure SMS Messaging Protocol			
8	TCAP, Transaction Capabilities Application Part			
Вариант 11				
1	ISDN, Integrated Services Digital Network			
2	IEEE 802.11 wireless LAN,			
3	RIP, Routing Information Protocol			
4	ISO-SP, OSI session-layer protocol (X.225, ISO 8327)			
5	XDR, eXternal Data Representation			
6	TDS, Tabular Data Stream			
7	TSP, Time Stamp Protocol			
8	VTP, Virtual Terminal Protocol			
Вариант 12				
1	SONET/SDH, Synchronous Digital Hierarchy, SONET			
2	LAPD, Link Access Procedures, D channel			
3	DDP, Datagram Delivery Protocol			

4	iSNS, Internet Storage Name Service			
5	X.25 Packet Assembler/Disassembler Protocol (PAD)			
6	Whois (and RWhois), Remote Directory Access Protocol			
7	WebDAV			
8	X.400, Message Handling Service Protocol			
Вариант 13				
1	802.11 Wi-Fi			
2	LocalTalk,			
3	BGP, Border Gateway Protocol			
4	L2F, Layer 2 Forwarding Protocol			
5	Telnet			
6	9P, Plan 9 from Bell Labs distributed file system protocol			
7	AFP, Apple Filing Protocol			
8	APPC, Advanced Program-to-Program Communication			
9	XMPP, Extensible Messaging and Presence Protocol			
Вариант 14				
1	Etherloop			
2	MPLS, Multiprotocol Label Switching			
3	Open Systems Interconnection (OSI) Model			
4	L2TP, Layer 2 Tunneling Protocol			

1	2	3	4	5
5	SSH Secure Shell			
6	AMQP, Advanced Message Queuing Protocol			
7	Atom Publishing Protocol			
8	Bitcoin – пиринговая система электронной наличности			
Вариант 15				
1	GSM Um radio interface			
2	PPP, Point-to-Point Protocol			
3	IPv4/IPv6, Internet Protocol			
4	NetBIOS, Network Basic Input Output System			
5	FTP, File Transfer Protocol			
6	CFDP, Coherent File Distribution Protocol			
7	CoAP, Constrained Application Protocol			
8	DDS, Data Distribution Service			
Вариант 16				
1	ITU и ITU-T			
2	SLIP, Serial Line Internet Protocol			
3	DVMRP, Distance Vector Multicast Routing Protocol			
4	PAP, Password Authentication Protocol			
5	TFTP, Trivial File Transfer Protocol			
6	ENRP, Endpoint Handlespace Redundancy Protocol			
7	FastTrack (KaZaa, Grokster, iMesh)			
8	Finger, User Information Protocol			
9	OSPF Open Shortest Path First			
Вариант 17				
1	TransferJet			
2	Spanning tree protocol,			
3	TCP, Transmission Control Protocol			
4	PPTP, Point-to-Point Tunneling Protocol			
5	SMTP, Simple Mail Transfer Protocol			
6	FTAM, File Transfer Access and Management			
7	Gopher, Gopher protocol			
8	HL7, Health Level Seven			
Вариант 18				
1	ARINC 818			
2	StarLan			
3	UDP, User Datagram Protocol			
4	RPC, Remote Procedure Call Protocol			
5	IMAP, Internet Mail Access Protocol			
6	H.323, Packet-Based Multimedia Communications System			
7	IRCP, Internet Relay Chat Protocol			
8	Kademlia			
9	DHCP Dynamic Host Configuration Protocol			
Вариант 19				
1	G.hn/G.9960			
2	Token ring,			

1	2	3	4	5
3	ARP, Address Resolution Protocol			
4	RTCP, Real-time Transport Control Protocol			
5	POP3, Post Office Protocol			
6	KAP, Anonymous File Transfer over UDP/IP (KickAss Protocol)			
7	LDAP, Lightweight Directory Access Protocol			
9	IS-IS, Intermediate System – Intermediate System			
Вариант 20				
1	USB, Universal Serial Bus			
2	ISDN, Integrated Services Digital Network			
3	ICMP, Internet Control Message Protocol			
4	SMPP, Short Message Peer-to-Peer			
5	HTTP, HyperText Transfer Protocol			
6	NFS, Network File System			
7	NIS, Network Information Service			
8	NNTP, Network News Transfer Protocol			
9	SPX Sequenced Packet eXchange			
Вариант 21				
1	Firewire			
2	x.25			
3	IGMP, Internet Group Management Protocol			
4	SCP, Session Control Protocol			
5	MIME (S-MIME), Multipurpose Internet Mail Extensions and Secure MIME			
6	Modbus			
7	Netconf			
8	NTCIP, National Transportation Communications for Intelligent Transportation System Protocol			

2.3 Лабораторная работа. Структура IP-адреса

Формат IP-адреса предполагает, что он состоит из двух логических частей – номера сети и номера узла в сети. Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла. Однако при передаче пакета по сети часто возникает необходимость разделить адрес на эти две части. Каким образом маршрутизаторы определяют, какая часть из 32 бит, отведённых под IP-адрес, относится к номеру сети, а какая – к номеру узла? Один из способов: разбиение всего цифрового поля 32 бит на пять классов адресов (RFC 791), где размеры сетей разные в каждом классе (рисунок 10). Три класса – A, B и C – предназначены для адресации сетей, а два – D и E – имеют специальное назначение.

Класс A. Адрес, в котором старший бит имеет значение 0. В этих адресах под идентификатор сети отводится 1 байт, а остальные 3 байта – это номер узла в сети.

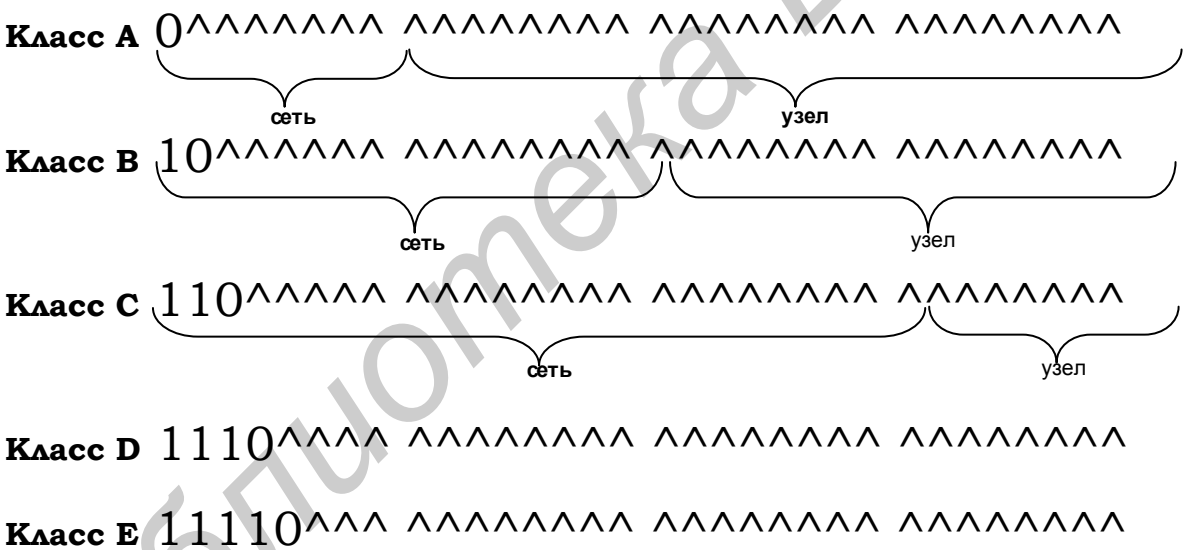


Рисунок 10 – Структура IP-адреса при разбиении на классы

Класс B. Адреса, старшие два бита которых имеют значение 10. В этих адресах номер сети и номер узла занимают 2 байта.

Класс C. Адреса, старшие три бита которых имеют значение 110. В этих адресах под номер сети отводится 3 байта, а под номер узла – 1 байт.

Класс D. Особый групповой адрес (multicast address).

Класс E. Адреса этого класса зарезервированы для будущих применений.

Упражнение для самостоятельной работы 9. *Определите число адресов* $N_{клA}$, $N_{клB}$, $N_{клC}$, $N_{клD}$, $N_{клE}$ *в каждом классе и напишите пограничные (граничащие с соседним классом) адреса. Сделайте это в десятеричной и шестнадцатеричной нотации.*

Упражнение для самостоятельной работы 10. *Сложите адреса и убедитесь, что сумма всех адресов во всех классах составит*

$$4\ 294\ 967\ 296\ \text{dec} = 1\text{oo}\ \text{ooo}\ \text{ooo}\ \text{hex} = 2^{32}.$$

Совпала ли сумма: $N_{клA} + N_{клB} + N_{клC} + N_{клD} + N_{клE}$ с вышеприведённым равенством 2^{32}, не нужно ли здесь ещё одно слагаемое: некое $N_{икс}$?

Упражнение для самостоятельной работы 11. *Определите, какое отношение* (*пропорцию*) *составят полученные адреса для всех пяти классов? Быть может, туда включить* $N_{икс}$?

$$N_{клA} : N_{клB} : N_{клC} : N_{клD} : N_{клE} = ? : ? : ? : ? : ?$$

Упражнение для самостоятельной работы 12. *Теперь определите число маршрутизируемых сетей и число узлов в сети для каждого класса. Этот расчёт необходимо делать, учитывая, во-первых, что часть адресов выделена под так называемые* ***частные*** *адреса*:

- в классе A – сеть **10.0.0.0**;
- в классе B – 16 сетей в диапазоне **172.16.0.0-172.31.0.0**;
- в классе C – 255 сетей **192.168.0.0-192.168.255.0**;

во-вторых, что в стеке TCP/IP существуют особые IP-адреса, то есть номер сети или номер узла не может состоять из одних двоичных нулей или единиц.

2.4 Лабораторная работа. Продвижение IP-пакетов в глобальной сети

2.4.1 Формирование DNS-запроса

Как продвигается пакет в составной сети, например на рисунке 11? Рассмотрим упрощённый вариант, считая, что узлы сети нашего примера имеют адреса, основанные на классах без масок. Как взаимодействует протокол IP с протоколами разрешения адресов ARP и DNS?

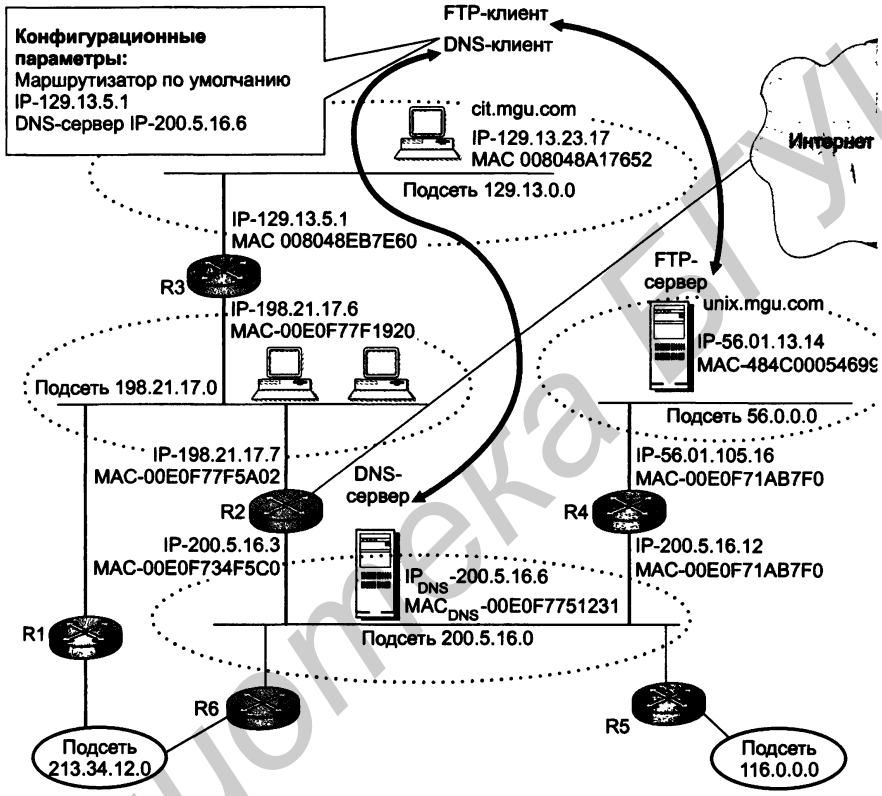


Рисунок 11 – Пример фрагмента составной сети одного домена – **mgu.com**

Пользователь компьютера cit.mgu.com, находящегося в сети 129.13.0.0, хочет установить связь с FTP-сервером. Пользователь знает символьное имя сервера unix.mgu.com, поэтому он набирает в браузере команду обращения к FTP-серверу по имени:

ftp://unix.mgu.com

Выполнение этой команды инициирует следующие операции:

– DNS-клиент cit.mgu.com обращается к ближайшему DNS-серверу 200.5.16.6 с запросом об IP-адресе сервера unix.mgu.com, с которым он хочет связаться;

– DNS-сервер, обработав запрос, передаёт ответ DNS-клиенту о найденном IP-адресе сервера unix.mgu.com;
– FTP-клиент cit.mgu.com, используя найденный IP-адрес сервера unix.mgu.com, формирует и передаёт сообщение на FTP-сервер.

Рассмотрим последовательно, как при выполнении этих операций взаимодействуют протоколы DNS, IP, ARP и Ethernet и что происходит при этом с кадрами и пакетами.

1. **Формирование IP-пакета с инкапсулированным в него DNS-запросом**.

Программный модуль FTP-клиента, получив команду

ftp unix.mgu.com,

передает запрос к работающей на этом же компьютере клиентской части протокола DNS, которая в свою очередь формирует к DNS-серверу запрос: «Какой IP-адрес соответствует символьному имени unix.mgu.com?» Запрос упаковывается в UDP-дейтаграмму, затем в IP-пакет. В заголовке пакета в качестве адреса назначения указывается IP-адрес 200.5.16.6 DNS-сервера. Этот адрес известен программному обеспечению клиентского компьютера, так как он входит в число его конфигурационных параметров. Сформированный IP-пакет будет перемещаться по сети в неизменном виде (рисунок 12), пока не дойдёт до адресата – DNS-сервера.

Рисунок 12 – Инкапсуляция дейтаграммы UDP с DNS-запросом в IP-пакет

2. **Передача кадра Ethernet с IP-пакетом маршрутизатору R3**. Для передачи этого IP-пакета необходимо его упаковать в кадр Ethernet, указав в заголовке MAC-адрес получателя. Протокол Ethernet способен доставлять кадры только тем адресатам, которые находятся в пределах одной локальной сети с отправителем. Если же адресат расположен не в этой подсети, то кадр надо передать ближайшему маршрутизатору для дальнейшего продвижения пакета. Для этого модуль IP, сравнив номера сетей в адресах отправителя и получателя, то есть 129.13.23.17 и 200.5.16.6 (см. рисунок 12), выяс-

няет, что пакет направляется в другую сеть, следовательно, его необходимо передать маршрутизатору. IP-адрес маршрутизатора по умолчанию также известен клиентскому узлу – он входит в число конфигурационных параметров.

Но для кадра Ethernet необходимо указать не IP-адрес, а MAC-адрес получателя. Это делает протокол ARP, который для ответа на вопрос: «Какой MAC-адрес соответствует IP-адресу 194.87.23.1?» – ищет соответствие в своей ARP-таблице. Поскольку обращения к маршрутизатору происходят часто, будем считать, что нужный MAC-адрес обнаружен в таблице и имеет значение 00:80:48:EB:7E:60. Теперь клиентский компьютер cit.mgu.com может отправить маршрутизатору R3 пакет, упакованный в кадр Ethernet (рисунок 13).

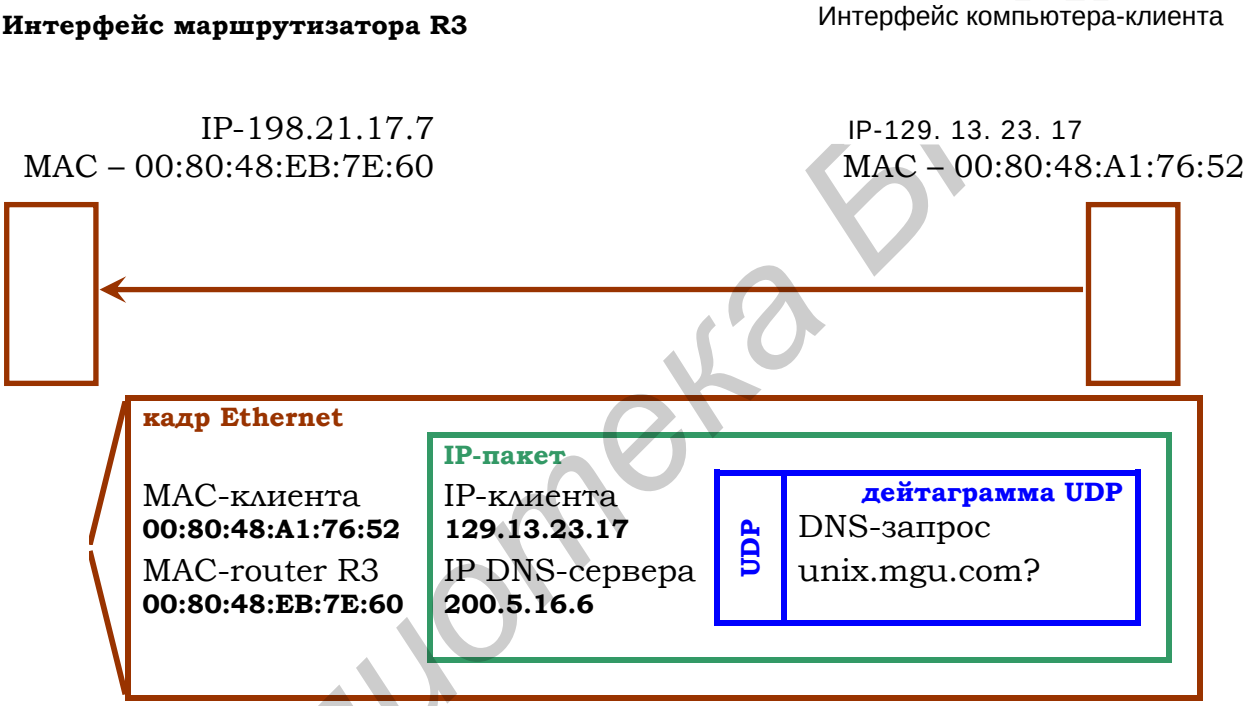


Рисунок 13 – Кадр Ethernet с инкапсулированным IP-пакетом, отправленный с клиентского компьютера

3. **Определение IP-адреса и MAC-адреса следующего маршрутизатора R2**. Кадр принимается интерфейсом 129.13.5.1 маршрутора R3. Протокол Ethernet, работающий на этом интерфейсе, извлекает из кадра IP-пакет и передаёт его протоколу IP. Протокол IP находит в заголовке пакета адрес назначения 200.5.16.6 и просматривает записи своей таблицы маршрутизации. Допустим маршрутизатор R3 не обнаруживает специфического маршрута для адреса назначения 200.5.16.6, но находит строку в своей таблице маршрутизации, адресующую в искомую сеть назначения:

200.5.16.0 198.21.17.7 198.21.17.6

Эта строка указывает, что пакеты для сети 200.5.16.0 маршрутизатор R3 должен передавать на свой выходной интерфейс 198.21.17.6, с которого они поступят на интерфейс следующего маршрутизатора R2, имеющего IP-адрес 198.21.17.7. Однако знания IP-адреса недостаточно, чтобы передать пакет по сети Ethernet. Необходим MAC-адрес маршрутизатора R2. Это работа протокола ARP и, если в ARP-таблице нет записи об адресе маршрутизатора R2, тогда в сеть отправляется широковещательный ARP-запрос, который поступает на все интерфейсы сети 198.21.17.0. Ответ приходит только от интерфейса маршрутизатора R2: «Я имею IP-адрес 198.21.17.7 и мой MAC-адрес 00:E0:F7:7F:5A:02». Теперь, зная MAC-адрес маршрутизатора R2 (00:E0:F7:7F:5A:02), маршрутизатор R3 отсылает ему IP-пакет с DNS-запросом (рисунок 14).

Упражнение для самостоятельной работы 13. *Нарисуйте по аналогии с рисунком* 14 *схему обмена кадрами Ethernet между маршрутизаторами R2 и R3 с инкапсулированными в них ARP-запросом и ARP-ответом. Объясните, как эта схема работает? Как вы считаете, если другой участник сети* 198.21.17.0 (*не маршрутизатор R3*), *тоже пожелает послать кадр на интерфейс* 198.21.17.7, *будет ли он формировать ARP-запрос? Почему*?

4. **Маршрутизатор R2 доставляет пакет DNS-серверу**. Модуль IP на маршрутизаторе R2 отбрасывает заголовок кадра Ethernet и извлекает из IP-пакета адрес назначения, просматривая свою таблицу маршрутизации. В ней он обнаруживает, что сеть назначения 200.5.16.0 непосредственно присоединена к его интерфейсу 200.5.16.3. Это означает, что пакет не нужно маршрутизировать, однако требуется определить MAC-адрес узла назначения. Протокол ARP, взаимодействуя с протоколом IP по схеме предыдущего пункта 3 и упражнения 13, определяет требуемый MAC-адрес 00:E0:F7:75:12:31 DNS-сервера. Получив ответ о MAC-адресе, маршрутизатор R2 отправляет в свою локальную сеть назначения кадр Ethernet с DNS-запросом (рисунок 15).

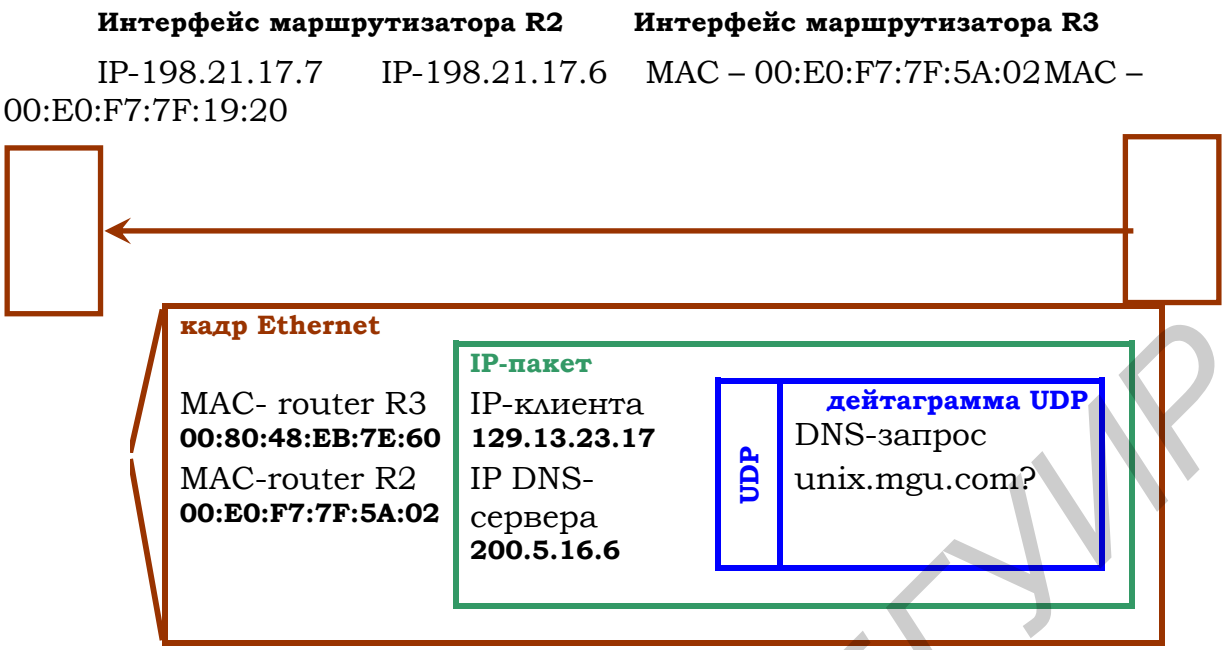


Рисунок 14 – Кадр Ethernet с DNS-запросом, отправленный с маршрутизатора R3 маршрутизатору R2

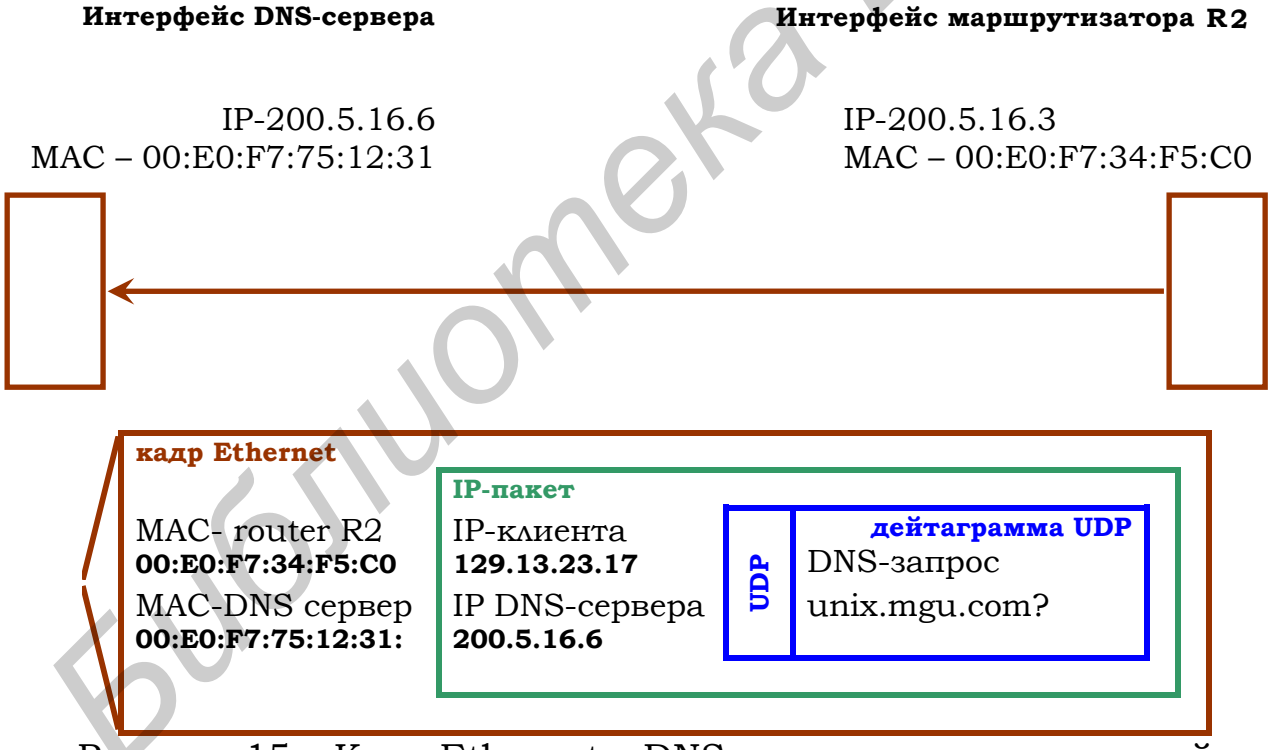


Рисунок 15 – Кадр Ethernet с DNS-запросом, отправленный с маршрутизатора R2

Упражнение для самостоятельной работы 14. *На рисунках* 13–15 *показаны три кадра Ethernet с инкапсулированными в них IP-пакетами, куда упакован соответствующий UDP-запрос с транспортного уровня. Создаётся впечатление, что все три* ***UDP-запроса***

должны быть одинаковы. Так ли это? Другими словами, одинакова ли контрольная сумма у ***UDP-запросов*** *в трёх кадрах Ethernet? Обоснуйте почему.*

Упражнение для самостоятельной работы 15. *На рисунках* 13–15 *показаны три кадра Ethernet с инкапсулированными в них IP-пакетами, куда упакован соответствующий UDP-запрос с транспортного уровня. Казалось бы, что все три* ***IP-пакета*** *должны быть одинаковы, потому что адрес назначения –* 200.5.16.6 *– и адрес источника –* 129.13.23.17 *– у них во всех трёх случаях одинаков. Так ли это? Другими словами, одинакова ли контрольная сумма у* ***IP-пакетов*** *в трёх кадрах Ethernet? Обоснуйте почему.*

Упражнение для самостоятельной работы 16. *На рисунках* 13–15 *показаны три кадра Ethernet с инкапсулированными в них IP-пакетами, куда упакован соответствующий UDP-запрос с транспортного уровня. Какие компоненты этих трёх* ***кадров Ethernet*** *постоянные, а какие переменные? Одинакова ли контрольная сумма у этих* ***кадров Ethernet****? Обоснуйте почему.*

2.4.2 Передача DNS-ответа

Наконец, DNS запрос прибыл на DNS-сервер и последний пятый шаг в этой цепочке событий продвижения пакета по составной сети описан в следующем пункте.

5. **Сетевой адаптер DNS-сервера принимает кадр Ethernet**, обнаруживает совпадение MAC-адреса назначения, содержащегося в заголовке, со своим собственным адресом и направляет его модулю IP. После анализа полей заголовка IP из пакета извлекаются данные вышележащих протоколов. DNS-запрос передаётся программному модулю DNS-сервера.

DNS-сервер просматривает свои таблицы, возможно, обращается к другим DNS-серверам и формирует ответ, смысл которого состоит в следующем: «Символьному имени Unix.mgu.com соответствует IP-адрес 56.01.13.14». Этот ответ DNS-сервера, спускаясь по интерфейсной части протоколов UDP, IP и Ethernet, в конце концов попадает на канальный уровень, где инкапсулируется в кадр протоколом Ethernet.

Путешествие IP-пакета с ответом через составную сеть в «обратную» сторону к компьютеру клиента осуществляется аналогично вышеописанным шагам: протоколы UDP, IP и Ethernet последовательно «заворачивают» ответ DNS-сервера в свои протокольные оболочки подобно вложенным друг в друга матрёшкам – это и называется инкапсуляцией. Последний шаг этого путешествия, от маршрутизатора R3 к компьютеру клиента, схематически изображён на рисунке 16.

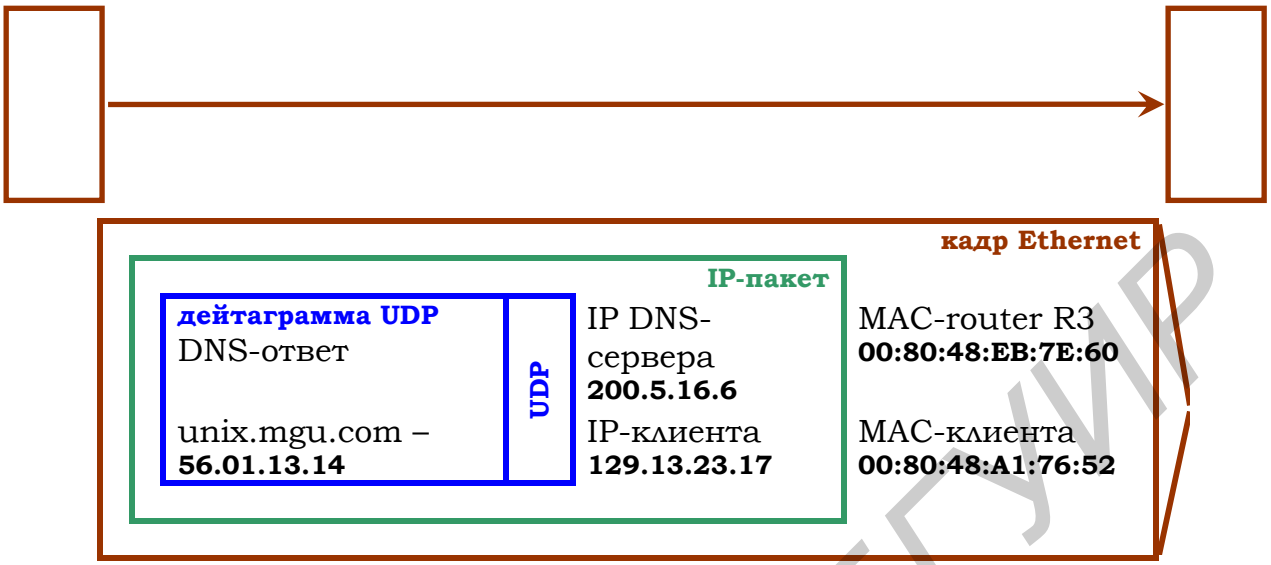


Рисунок 16 – Кадр Ethernet с DNS-ответом, отправленный с маршрутизатора R3 компьютеру-клиенту

2.4.3 Передача пакета от FTP-клиента к FTP-серверу

FTP-клиент, получив IP-адрес FTP-сервера, посылает ему своё сообщение, используя те же механизмы доставки данных через составную сеть, как и рассмотренные нами выше.

Упражнение для самостоятельной работы 17. *Опишите процесс передачи пакета к FTP-серверу, обращая внимание на значения адресных полей заголовков кадров и заголовка вложенного IP-пакета.*

Упражнение для самостоятельной работы 18. *Изобразите диаграммы продвижения пакетов как на рисунках* 13–15 *для первого* – 129.13.0.0 – *и последнего* – 56.0.0.0 – *сегментов составной сети.*

Упражнение для самостоятельной работы 19. *Объясните: почему на рисунках 12–16 все адресные поля кадров Ethernet разные, а адресные части заголовков IP-пакетов с адресами назначения и адресами источника – одинаковые?*

Упражнение для самостоятельной работы 20. *На рисунке 11 представлен фрагмент глобальной сети, где показаны четыре локальные подсети. Определите классы IP-адресов в показанных сетях; номер самой сети и заполните этими данными два пустых поля таблицы 8, считая, что маски в этом фрагменте сети не используются.*

Таблица 8 – Соответствие классов IP-адресов сетям и интерфейсам устройств

Устройство	**IP-адрес интерфейса**	**IP-адрес сети**	**Класс IP-адреса**
Компьютер клиента	129.13.23.17		
Маршрутизатор R2	198.21.17.7		
Маршрутизатор R2	200.5.16.3		
Маршрутизатор R3	198.21.17.6		
Маршрутизатор R3	129.13.5.1		
DNS-сервер	200.5.16.6		
Маршрутизатор R4	56.1.105.16		
FTP-сервер	56.1.13.14		
Маршрутизатор R4	200.5.16.12		
Маршрутизатор R1	213.34.12.3		
Маршрутизатор R1	198.21.17.5		
Маршрутизатор R5	116.02.13.29		
Маршрутизатор R5	200.5.16.4		

Подсказка. *Какой должен быть префикс первого байта IP-адреса в зависимости от класса сети*?

2.4.4 Структуризация сети масками одинаковой длины

Алгоритм маршрутизации усложняется, когда в систему адресации узлов вносятся дополнительные элементы – маски. Причина отказа от метода адресации, основанного на классах, – потребность в структуризации сетей и ликвидация нераспределённых номеров сетей в условиях дефицита IP-адресов.

Использование масок позволяет разделить одну сеть на несколько (рисунок 17).

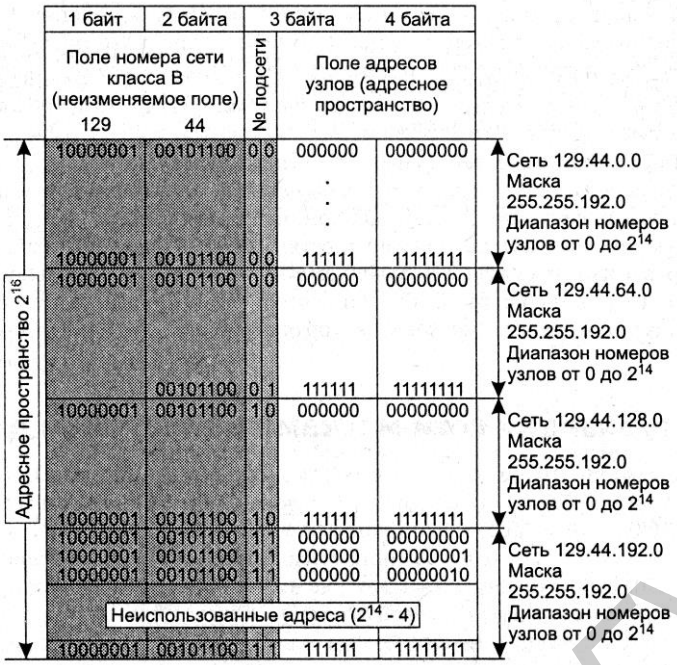


Рисунок 17 – Разделение сети 129.44.0.0 **класса B** на четыре более мелкие с помощью масок

Изначально у нас есть сеть класса B: 129.44.0.0 – это одна большая неструктурированная сеть с 2^{16} узлами, но нам необходимо несколько отдельных, маленьких подсетей, чтобы трафик в каждой подсети был локализован. Такую сеть легче диагностировать и проводить в каждой из подсетей свою политику безопасности [3]. Разделение большой сети с помощью масок позволяет скрыть внутреннюю структуру сети от внешнего наблюдения.

На рисунке 17 показано разделение всего адресного диапазона на 4 равные части – каждая по 2^{14} адреса. При этом число разрядов, доступное для нумерации узлов, уменьшилось на два бита, а префикс (номер) каждой из четырех сетей стал длиннее на два бита. Каждый из четырёх диапазонов можно записать в виде IP-адреса с маской, состоящей из 18 единиц, или в десятичной нотации – 255.255.192.0.

Пример сети, построенной путём деления на 4 сети равного размера, показан на рисунке 18. Весь трафик во внутреннюю сеть 129.44.0.0 из внешней сети поступает через маршрутизатор R1. Для структуризации во внутренней сети установлен дополнительный маршрутизатор R2. Каждая из вновь образованных сетей 129.44.0.0/18, 129.44.64.0/18, 129.44.128.0/18 и 129.44.192.0/18 подключена к портам внутреннего маршрутизатора R2.

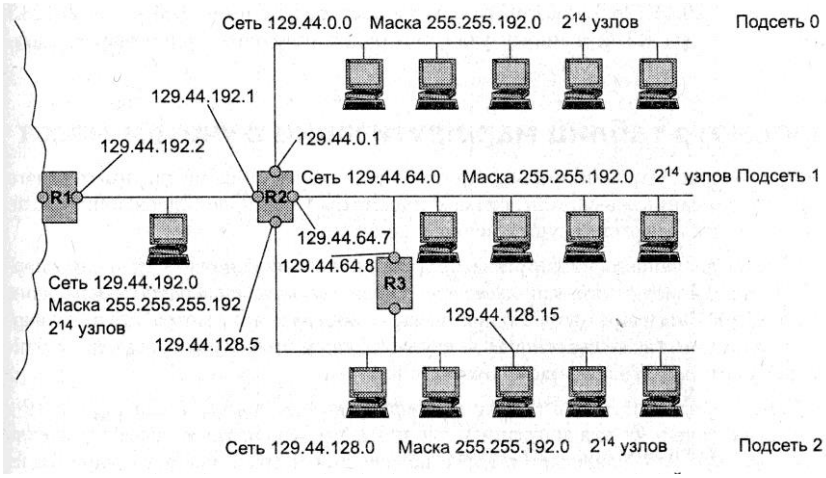


Рисунок 18 – Пример построения маленьких сетей из одной большой **класса B** с использованием маски постоянной длины

В сети 129.44.192.0/18, соединяющей маршрутизаторы R1 и R2, для адресации узлов задействованы всего два IP-адреса – 129.44.192.1 и 129.44.192.2 – это порты маршрутизаторов R1 и R2. Остальные из 2^{14} IP-адресов этой подсети не используются. Этот пример показывает неэффективность сетей равного размера, а следовательно, неэффективность масок одинаковой длины.

Извне сеть по-прежнему выглядит как единая сеть класса B. Однако поступающие в сеть IP-пакеты разделяются маршрутизатором R2 между четырьмя подсетями. В этой сети механизм классов не действует и маршрутизатор должен иметь другое средство, позволяющее ему определять, какая часть IP-адреса, помещённого в поле адреса назначения, является номером сети. Эта часть из IP-адреса вычленяется с помощью маски и логической операции конъюнкции. Маска является важнейшим компонентом процесса маршрутизации и её значение включено во второе поле таблицы маршрутизации R2 (таблица 9).

Таблица 9 – Таблица маршрутизации R2 с масками одинаковой длины

Адрес назначения	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.192.0	129.44.0.1	129.44.0.1	Подключена
129.44.64.0	255.255.192.0	129.44.64.7	129.44.64.7	Подключена
129.44.128.0	255.255.192.0	129.44.128.5	129.44.128.5	Подключена
129.44.192.0	255.255.192.0	129.44.192.1	129.44.192.1	Подключена
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	–
129.44.128.15	255.255.255.255	129.44.64.8	129.44.64.7	–

Первые четыре записи в таблице 9 соответствуют внутренним подсетям, непосредственно подключённым к портам маршрутизатора R2. Запись 0.0.0.0 с маской 0.0.0.0 соответствует маршруту по умолчанию. Последняя запись определяет так называемый специфический маршрут к узлу 129.44.128.15.

Упражнение для самостоятельной работы 21. *Составьте две свои таблицы маршрутизации, аналогичные таблице 9, для маршрутизаторов R1 и R3* (см. *рисунок 18*) *с масками постоянной длины. Куда вы распорядились бы с этих маршрутизаторов отправлять пакеты по умолчанию? Отобразите ваше пожелание строкой записи в вашей новой таблице маршрутизации.*

Упражнение для самостоятельной работы 22. *Значения IP-адресов в третьем* (**Адрес следующего маршрутизатора**) *и четвёртом* (**Адрес порта**) *столбцах таблицы маршрутизации иногда совпадают, а иногда нет. Чем обусловлено совпадение* (*или* ***не***совпадение). *Или это ошибка? Объясните.*

Упражнение для самостоятельной работы 23. *На маршрутизатор R2 прибыл пакет с адресом* 129.44.78.200. *Опишите его и определите, в какую подсеть будет направлен этот пакет. Как вычленить из IP-адреса* 129.44.78.200 *номер сети и номер конечного узла? Проделайте это.*

2.4.5 Определение «наружных» параметров локальной сети, подключённой к глобальной сети

В настоящее время можно считать укоренившейся практикой употребление в локальных сетях немаршрутизируемых частных адресов. Употребление частных адресов позволяет экономить «настоящие» IP-адреса. Трансляцию частных IP-адресов в «настоящие» осуществляет сервис перевода адресов NAT (Network Address Translation). Обычно этот сервис соседствует с сервисом Proxy и устанавливается на пограничном сервере на краю локальной сети.

Иногда нам, находясь внутри локальной сети, необходимо узнать «наружные», внешние параметры локальной сети: IP-адрес, доменное имя, номер автономной системы, поставщика интернет-услуг. Не имея доступ к пограничному серверу и конфигурационным параметрам NAT, сделать это затруднительно.

В таких случаях можно воспользоваться услугами сторонних разработчиков, бесплатно размещающих такие приложения на своих web-страничках. Одно из таких приложений, которое мы разберём, находится по адресу: http://2ip.ru (рисунок 19). На этой web-странице предлагается обширный перечень бесплатных тестов и сервисов, к примеру:

– информация об IP-адресе и домене;
– DNS-параметры домена;
– расстояние до сайта;
– проверка порта;
– безопасность вашего компьютера.

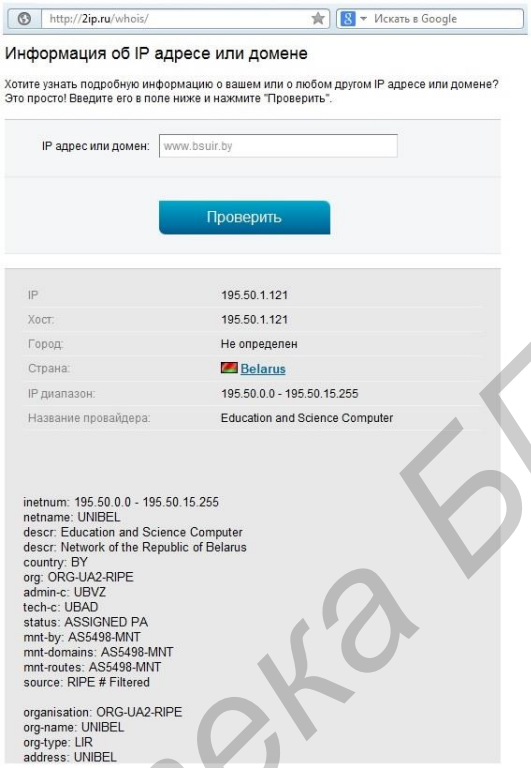


Рисунок 19 – Поисковое приложение с web-страницы http://2ip.ru

Упражнение для самостоятельной работы 24. *На рисунке 19 представлена «наружная» информация о сайте нашего вуза* http://bsuir.by, *полученная из* http://2ip.ru/whois/. *Освежите на своём компьютере данные этой web-страницы и определите следующее*:

– *«наружный» IP-адрес*;
– *диапазон и количество IP-адресов, которыми владеет БГУИР*;
– *удостоверьтесь, что страна-резидент – Belarus*;
– *провайдера БГУИР*;
– *номер автономной системы, куда включён БГУИР.*

Упражнение для самостоятельной работы 25. *Как бы вы распорядились, используя диапазон адресов на рисунке 19, при построении сети нашего вуза? Создайте проект такой сети, используя маски переменной длины и учитывая следующие обстоятельства:*

- *необходима внутренняя подсеть с учебными классами для студентов;*
- *необходима внутренняя подсеть для учебных кафедр;*
- *необходима внутренняя подсеть для администрации;*
- *необходима подсеть в демилитаризованной зоне для размещения внешней web-страницы вуза и других внешних ресурсов с угрозой внешнего вторжения.*

Упражнение для самостоятельной работы 26. *Проработайте упражнение 24, находясь у себя дома или в общежитии. Выполните перечисленные в нём задания. Сравните и проанализируйте полученные здесь результаты с теми, которые получились у вас в упражнении 24.*

Найдите с помощью поисковых систем аналог приложения http://2ip.ru/ *и выполните задания из упражнения 24. Сравните полученные результаты.*

2.5 Лабораторная работа. Протокол ICMP. Работа с утилитами tracert и ping

Протокол IP доставляет данные, руководствуясь принципом «по возможности», и не предпринимает мер для гарантированной передачи данных адресату. Свойство «необязательности» протокола IP компенсируется протоколами более высоких уровней на транспортном уровне.

Встречается ряд ситуаций, когда протокол IP не может доставить пакет адресату. В этом случае приходят на выручку возможности, предоставляемые протоколом ICMP (Internet Control Message Protocol). Этот вспомогательный, но полезный протокол работает на сетевом уровне совместно с основным протоколом IP и используется для диагностики сети.

Протокол ICMP служит дополнением, компенсирующим ненадёжность протокола IP. Он не предназначен для восстановления потерянных при передаче пакетов: если пакет потерян, ICMP не может послать его заново. Но протокол ICMP может оповестить отправителя об ошибках, произошедших при передаче его пакетов.

Сообщения об ошибках протокола ICMP лежат в основе работы утилиты **traceroute** ОС Linux (в Windows она называется **tracert**). Эта утилита позволяет проследить маршрут до удалённого хоста, IP-адрес и доменное имя каждого промежуточного маршрутизатора. Эта информация помогает найти маршрутизатор, на котором обрывается путь пакета к удалённому хосту.

Выполните упражнения 27–29, предложенные ниже, используя диагностические утилиты **traceroute** и **tracert**.

Замечание. Следует иметь в виду, что утилита **traceroute** в ОС Linux по умолчанию проводит трассировку маршрута, используя дейтаграммы UDP, что позволяет работать с утилитой обычному пользователю, так как реализация UDP в Linux поддерживает так называемые ошибки очереди, через которые ошибки ICMP-пакетов могут поставляться в пользовательское приложение.

Если у вас трассировка маршрута не получается по умолчанию, попытайтесь набрать в командной строке команду с ключом **-I**, например так:

traceroute -I en.wikipedia.org

С этим ключом команда **traceroute** отправляет на узел назначения эхо-пакеты ICMP. Но с ключом **-I** Linux может потребовать от вас привилегий суперпользователя. Напомним также, что как и ключи, так и синтаксис команд в ОС Linux чуствителен к регистру написания символов.

Упражнение для самостоятельной работы 27. Используя консольную утилиту traceroute (tracert), освежите значения и заполните недостающие записи в таблице 10. Определите соответствие до-

менного имени и IP-адреса, цепочку маршрутизаторов, по которым прокладывается маршрут, и задержку в каждом узле.

Таблица 10 – Разрешение доменных имён и IP-адресов

№ п/п	IP-адрес	Доменное имя	Ресурс
1	212.98.168.51	www.sb.by	Советская Белоруссия
2	93.85.84.179	minsk.gov.by	?
3	178.124.133.66	www.tut.by	?
4	91.149.157.62	www.pravo.by	?
5	212.98.162.9	www.nbrb.by	?
6	81.19.85.116	lenta.ru	?
7	195.50.1.121	www.bsuir.by	БГУИР
8	91.149.157.152	www.informatics.by	?

Как вы думаете, почему если к доменным именам некоторых нагруженных сайтов применить несколько раз подряд утилиту **traceroute**, *то можно получить разные IP-адреса*?

Замечание. Для определения соответствия доменного имени IP-адресам можно воспользоваться командой **nslookup**. Набрав в командной строке

nslookup www.tut.by,

мы получим список IP-адресов (или всего один IP-адрес), которыми владеет искомый домен.

Упражнение для самостоятельной работы 28. *Проработайте упражнение 27, находясь у себя дома или в общежитии. Выполните перечисленные в нём задания. Сравните и проанализируйте полученные здесь трассы маршрутов с маршрутами, которые получились у вас в упражнении 27 в компьютерном классе БГУИР.*

Рассмотрим ещё одну полезную консольную утилиту, часто используемую для диагностики сети, – это команда **ping**. Её можно применять для диагностики как в локальной сети, так и в составной глобальной. Эта команда тоже использует ICMP-сообщения – эхо-запросы и эхо-ответы.

Эхо-запрос и эхо-ответ, в совокупности называемые **эхо-протоколом**, представляют собой простое средство мониторинга сети. Компьютер посылает по сети ICMP-сообщение эхо-запроса, указывая в нем IP-адрес узла, достижимость которого нужно проверить. Узел, получивший эхо-запрос, формирует и отправляет эхо-ответ отправителю запроса.

Эхо-запрос и эхо-ответ передаются по сети внутри IP-пакетов, и их успешная доставка (выполнение команды **ping**) означает нормальное функционирование всей транспортной системы составной сети, всего кабельного хозяйства и более того – работоспособность первых трёх уровней, включая сетевой. Если в этом случае пользователь испытывает проблемы с работой сети, то это можно отнести только к сбоям программного обеспечения.

В противном случае, когда команда **ping** сообщает «Заданный узел недоступен» или «Destination Host Unreachable», – это означает сбой или поломку аппаратуры: отсутствие соединения (обрыв кабеля, отключена аппаратура, отсутствует сигнал); поломку сетевого адаптера или ненадлежащую его работу.

Упражнение для самостоятельной работы 29. *Пропингуйте IP-адреса из таблицы упражнения 27. Какие получились результаты? Узнайте у вашего соседа-студента в компьютерном классе IP-адрес его компьютера, запустив утилиту* **ipconfig /all**. *Сообщите соседу IP-адрес своего компьютера. Пропингуйте компьютеры друг друга.*

2.6 Лабораторная работа. Маршрутизация с масками. Перекрытие адресных пространств

Практика показала, что более эффективным является разбиение сети на подсети разного размера. Для неудачного решения подсети на рисунке 19 – 129.44.192.0 – где «пропало» 2^{14} IP-адреса, и которая связывает два маршрутизатора по двухточечной схеме, даже количество адресов сети класса С является избыточным.

Сложность использования масок возникает уже на этапе проектирования сети, которое включает:

- определение количества сетей, из которых будет состоять вся сеть;
- оценку требуемого количества адресов для каждой сети;
- получение диапазона адресов от поставщика услуг;
- распределение адресного пространства между сетями.

Покажем пример использования масок при построении сети с перекрывающимися адресными пространствами.

Эта сеть изображена на рисунке 20. Какой для неё необходим диапазон IP-адресов? Она состоит из трёх подсетей. Две из них – это защищённые от внешних атак внутренние подсети отделов: сеть Ethernet на 600 пользователей и сеть Token Ring на 200 пользователей. Для проектируемой сети предусмотрены внешние ресурсы открытого доступа (web-серверы, FTP-серверы) для «наружных» клиентов.

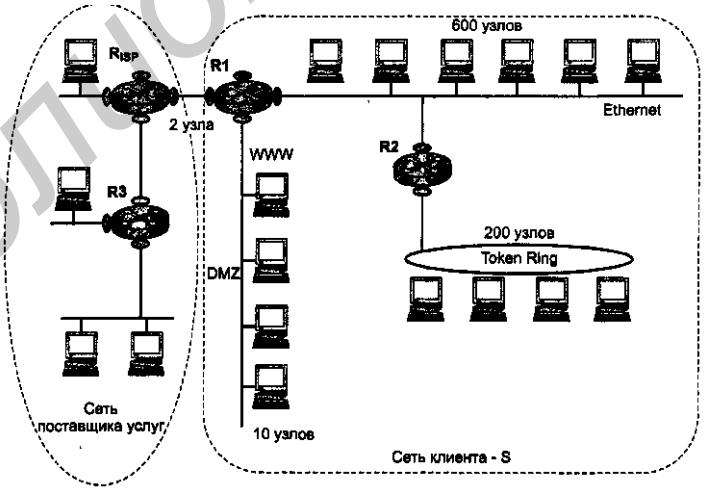


Рисунок 20 – Планируемая сеть клиента

Участки корпоративной сети, планируемые как источники публичной информации, называют **демилитаризованной зоной** (Demilitarized Zone, DMZ).

Ещё одна сеть на два узла потребуется для связи с поставщиком услуг, то есть общее число адресов, требуемых для адресации сетевых интерфейсов, составляет 812. Четвёртая подсеть необходима, чтобы диапазон доступных адресов включал для каждой из подсетей широковещательные адреса, состоящие только из единиц или только из нулей. Исходя из вышесказанного минимальное число адресов, необходимое для построения задуманной сети, превышает значение 812, полученное простым суммированием узлов.

Вариант возможного диапазона адресов поставщика услуг изображён на рисунке 21. Клиенту предложено выделенное зелёным адресное пространство. Это непрерывный диапазон 1024 адресов. Значение 1024 выбрано как наиболее близкое к требуемому количеству адресов, равное степени двойки (2^{10} = 1024). Выделяемое адресное пространство ложится на уже распределённые адреса поставщика услуг.

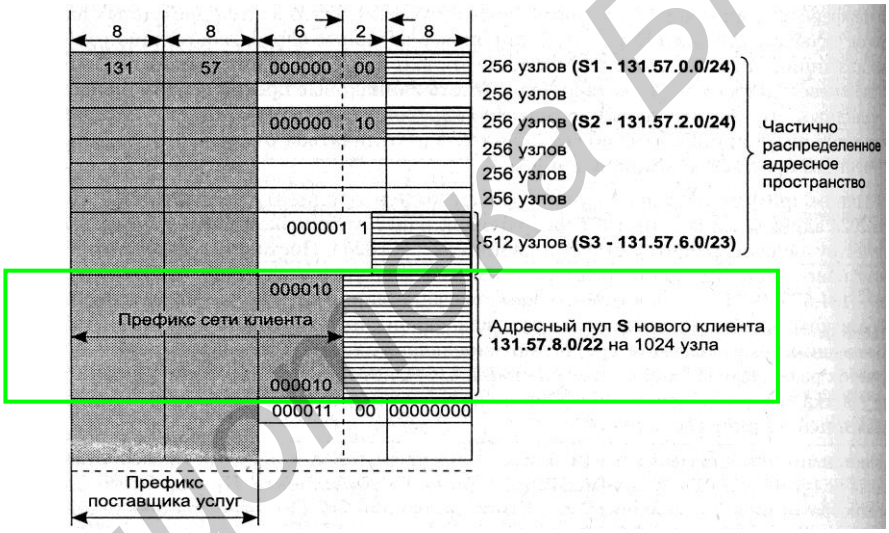


Рисунок 21 – Адресное пространство поставщика услуг

Один из вариантов распределения, полученного от поставщика услуг адресного пространства S между четырьмя подсетями, представлен на рисунке 22. Для самой большой сети Ethernet на 600 узлов выделяем весь диапазон адресов 131.57.8.0/22, полученный от поставщика услуг. Номер этой сети совпадает с номером сети, полученным от поставщика услуг.

Но осталось ещё три подсетки. Поскольку для сети Ethernet требуется только 600 адресов, то из оставшихся 624 (1024 – 600 = 624) строим сеть Token Ring 131.57.9.0/24 на 250 адресов. Но для Token Ring требуется только 200 адресов, вот почему из 250 адресов можно выделить ещё два диапазона: для сети DMZ 131.57.9.16/28 на

16 адресов и для связывающей сети 131.57.9.32/30 на 4 адреса. Теперь все подсети получили достаточное количество адресов.

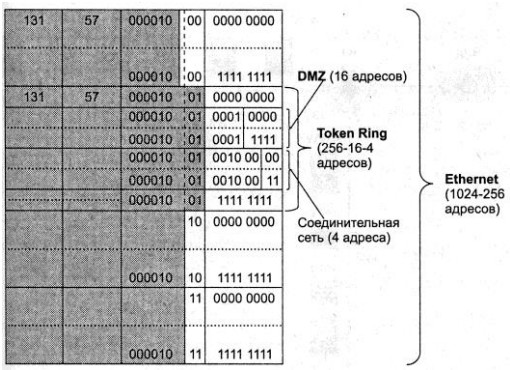


Рисунок 22 – Планируемый диапазон адресов для проектируемой сети

Упражнение для самостоятельной работы 30. *Как вы думаете, остались ли после построения сети S* (*рисунок 23*) *у сисадмина «в запасе» свободные адреса? Покажите на схеме* (*см. рисунок 22*) *диапазоны, где они могут быть. Какие маски соответствуют этим диапазонам?*

Следующий этап – это конфигурирование сетевых интерфейсов конечных узлов и маршрутизаторов. Каждому интерфейсу сообщается его IP-адрес и соответствующая маска. После распределения адресного пространства сеть клиента будет выглядеть, как показано на рисунке 23. После конфигурирования сетевых интерфейсов должны быть созданы таблицы маршрутизации маршрутизаторов R1 и R2 клиента. В таблице 11 представлены маршруты маршрутизатора R2.

Таблица 11 – Таблица маршрутизации R2

Адрес назначения	Маска	След. маршрут	Вых. интерфейс	Метрика
131.57.8.0	255.255.252.0	131.57.8.2	131.57.8.2	Подключена
131.57.9.0	255.255.252.0	131.57.9.1	131.57. 9.1	Подключена
131.57.9.16	255.255.252.240	131.57.8.1	131.57.8.2	1
131.57.9.32	255.255.252.252	131.57.8.1	131.57.8.2	1

В данной таблице нет маршрута по умолчанию, поэтому все IP-пакеты, адресованные сетям, адреса которых явно не указаны в таблице, будут отбрасываться маршрутизатором. В изложенном методе с

перекрытием адресных пространств возникает кажущееся противоречие.

Казалось бы, IP-пакет, адресованный в демилитаризованную зону, «застрянет» в сети Token Ring (см. рисунок 22), поскольку его IP-адрес как раз накрывает диапазон IP-адресов подсети Token Ring. Как же всё это работает?

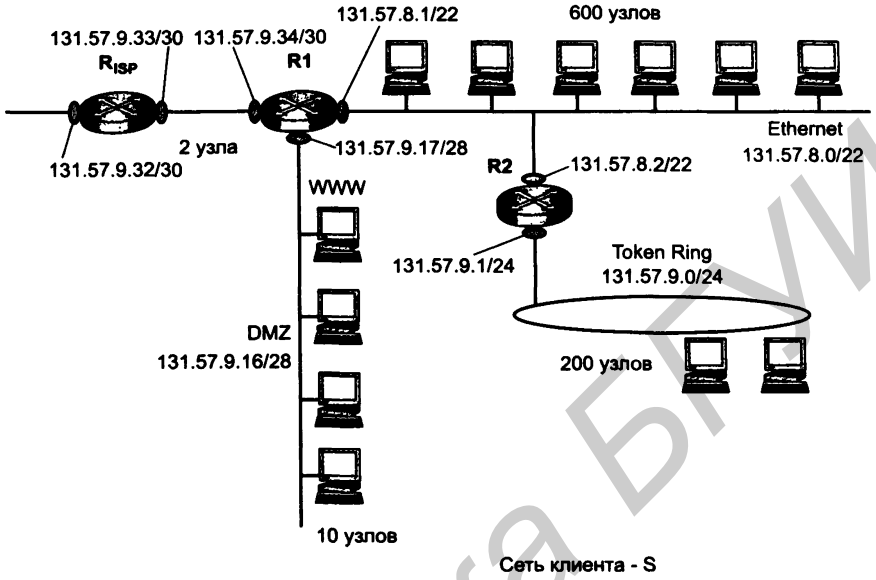


Рисунок 23 – Сконфигурированная сеть клиента S

Пусть, действительно, на маршрутизатор R2 поступает пакет с адресом назначения **131.57.9.29**. Проанализируем, как маршрутизатор обработает этот пакет с использованием масок:

(**131.57.9.29**) & (**255.255.252.0**)	= **131.57.8.0**	совпадение;
(**131.57.9.29**) & (**255.255.255.0**)	= **131.57.9.0**	совпадение;
(**131.57.9.29**) & (**255.255.255.240**)	= **131.57.9.16**	совпадение;
(**131.57.9.29**) & (**255.255.255.252**)	= **131.57.9.28**	нет совпадения.

Получено три совпадения. Вспомним алгоритм просмотра таблиц маршрутизации с масками (пункт 1.6.2), где четвёртое правило гласит: «*в случае **нескольких** совпадений все помеченные строки сравниваются и выбирается тот маршрут, в котором количество совпавших разрядов наибольшее*». В результате операции конъюнкции видно, что наибольшее количество совпавших двоичных разрядов в третьей строке – 28 разрядов, тогда как в первой строке их всего 22, а во второй – 24. Следовательно, маршрутизатор R2, согласно алгоритму просмотра таблиц, выберет сеть **131.57.9.16** из третьей строки, которая соответствует демилитаризованной зоне, и направит туда пакет с адресом **131.57.9.29.**

Упражнение для самостоятельной работы 31. *Предложите свой, на ваш взгляд, оптимальный вариант построения сети S с перекрытием адресного пространства, изображённой на рисунке 23. Опишите его, постройте схему и диаграмму с необходимыми масками переменной длины. Если вы считаете, что представленный вариант распределения адресного пространства* ***единственный****, то обоснуйте «почему»? Для выполнения этого упражнения воспользуйтесь своими результатами из упражнения* 25.

Упражнение для самостоятельной работы 32. *В тексте приведена таблица маршрутизации для* R2. *Постройте таблицы маршрутизации для маршрутизаторов* R1 и R_{ISP}. *Создайте в этой таблице строку для специфического маршрута к одному из узлов сети* **131.57.9.0** – *Token Ring. Создайте в таблице строку для маршрута по умолчанию на интерфейс* **131.57.9.32** *маршрутизатора* R_{ISP}. *Какие в этих строках будут маски*?

Упражнение для самостоятельной работы 33. *Постройте сеть* S [5] *с перекрытием адресных пространств, для следующих случаев*:

сеть Ethernet	300	адресов;
сети Token Ring	30	адресов;
демилитаризованная зона	20	адресов;
соединительная сеть	8	адресов.

Какой диапазон адресов необходимо получить у поставщика услуг на этот раз? Как сисадмин распределит адреса между этими четырьмя сетями? Как будут выглядеть таблицы маршрутизации R1 *и* R2?

Упражнение для самостоятельной работы 34. *Если вы успешно справились с упражнением 31, постройте таблицы маршрутизации для вашего варианта сети.*

2.7 Лабораторная работа. Сети на основе Wi-Fi (Wireless Fidelity). Реализация Wi-Fi сети

2.7.1 Требования к работе

Целью этой лабораторной работы является изучение беспроводных сетей и их применения на практике. Этот проект должен содержать:

- организацию беспроводной сети в замкнутом пространстве;
- определение режима работы сети – Ad-hoc (точка-точка) или клиент-сервер;
- обоснование и выбор типа шифрования;
- определение топологии сети;
- описание настройки оборудования для реализации варианта построения Wi-Fi сети.

2.7.2 Варианты заданий

Варианты построения Wi-Fi сети. Необходимо выбрать один из следующих вариантов.

1. Настроить точку доступа Wi-Fi на планшете. Подключить смартфон к созданной точке доступа Wi-Fi. Показать работу на примере копировании файлов с планшета на смартфон и обратно.
2. Настроить точку доступа Wi-Fi на планшете. Подключить смартфон к созданной точке доступа Wi-Fi. Продемонстрировать работу в Internet на смартфоне через созданную точку доступа Wi-Fi.
3. Подключить смартфон к Nootbook, имеющему Wi-Fi, как Modem. Создать точку доступа с парольным доступом для подключения к Internet.
4. Настроить точку доступа Wi-Fi на смартфоне. Подключить к созданной точке доступа Wi-Fi планшет. Показать работу на примере копировании файлов с планшета на смартфон и обратно.
5. Настроить точку доступа Wi-Fi на смартфоне. Подключить к созданной точке доступа Wi-Fi планшет. Продемонстрировать работу в Internet на планшете через созданную точку доступа Wi-Fi.
6. Настроить точку доступа Wi-Fi на смартфоне с использованием 3G для доступа в Internet. Подключить к созданной точке доступа Wi-Fi планшет. Продемонстрировать работу в Internet на планшете через созданную точку доступа Wi-Fi.
7. Настроить точку доступа Wi-Fi на планшете с использованием 3G для доступа в Internet. Подключить к созданной точке доступа Wi-Fi смартфон. Продемонстрировать работу в Internet на смартфоне через созданную точку доступа Wi-Fi.

8. Decktop-компьютер, подключённый к локальной сети БГУИР + Wi-Fi modem. Создать точку доступа с парольным доступом для подключения к Internet.
9. Nootbook с Wi-Fi, подключённый к локальной сети БГУИР. Создать точку доступа с парольным доступом для подключения к Internet.
10. Decktop-компьютер, подключённый к локальной сети БГУИР и маршрутизатору с Wi-Fi доступом, также подключённым к локальной сети БГУИР. Настроить общий доступ к Internet.
11. Decktop-компьютер, подключённый к локальной сети БГУИР и маршрутизатору с Wi-Fi доступом, также подключённым к локальной сети БГУИР. Настроить подключение SmartTV телевизора , имеющего Wi-Fi.
12. Планшет с Wi-Fi, подключённый к локальной сети БГУИР. Организовать подключение SmartTV телевизора, имеющего Wi-Fi.
13. Nootbook с Wi-Fi, подключённый к локальной сети БГУИР. Организовать подключение SmartTV телевизора, имеющего Wi-Fi.
14. Выбрать необходимое оборудование и реализовать просмотр программ Online TB на SmartTV телевизоре.
15. Выбрать необходимое оборудование и реализовать просмотр программ Online TB на SmartTV телевизоре, имеющем Wi-Fi.

2.8 Лабораторная работа. Создание проекта компьютерной сети

2.8.1 Требования к работе

Требуется разработать проект небольшой локальной компьютерной сети от 5 до 50 клиентских машин. Этот проект должен содержать:

- отображение топологии сети (схема сети);
- проработку схемы внутренних соединений;
- выбор типа связи с глобальной сетью;
- оценку внутреннего и внешнего трафика;
- обоснование выбора оборудования;
- спецификацию со ссылками на сайты производителей;
- выбор программного обеспечения;
- обоснование и реализацию системы безопасности проектируемой сети;
- привязку компонентов оборудования к 7-уровневой модели OSI;
- оценку примерной стоимости оборудования такой сети.

2.8.2 Варианты заданий

Предлагается выбрать один из вариантов построения компьютерной сети в зависимости от его предпочтений.

1. Недорогая бюджетная сеть рекламного офиса с 10 сотрудниками.
2. Семейная сеть средней стоимости: у одного члена семьи Notebook, у всех остальных – компьютеры.
3. Мультимедийная сеть (домашний кинотеатр, «цифровой дом»).
4. Игровая сеть мальчишек вашего подъезда.
5. Компьютерная сеть для обслуживания обширной электронной библиотеки кафедры. «Живые» книжки – отсутствуют; абонентская часть – отсутствует.
6. Компьютерная сеть для обслуживания обширной библиотеки кафедры с электронными и «живыми» книжками. Есть абонентская часть.
7. Сеть для построения и вывода изображения большого размера (4 × 5 метров) на большой составной (ячеистый) экран, например, смонтированный на стене здания.
8. Сеть для бригады системных программистов из 12 человек с начальником (низкоуровневое программирование, Assembler, C, C++).
9. Сеть для бригады системных программистов из 10 человек для разработки кроссплатформенных приложений.
10. Сеть для бригады программистов-разработчиков из 15 человек (среды визуального программирования Delphi, Visual Studio).

11. Сеть для бригады программистов из 10 человек с координатором-постановщиком (web-дизайн, создание сайтов для организаций в Интернете).
12. Мобильная сеть для взлома с 5 хакерами, ноутбуки, мобильные телефоны (GAS, Assembler, отладчики SoftICE, дизассемблеры IDA Pro, декомпиляторы, мониторы, сетевые анализаторы пакетов).
13. Сеть для монтажников-телевизионщиков (10 человек с режиссёром-постановщиком) для производства и монтажа мультфильмов, сборки и монтажа кинофильмов и телефильмов.
14. Семейная сеть «ни в чём себе не отказывай»: компьютеры у всех членов семьи.
15. Сеть с сервером для разработчиков баз данных.
16. Сеть небольшого предприятия – 50 сотрудников (файловый сервер, почтовый сервер, сервер печати, поддержка пакета «Бухгалтерия», поддержка пакета «Кадры»)
17. Сеть с сервером баз данных, поддерживающая режим работы клиент/сервер.
18. Сеть рассредоточенного предприятия (4 производственные площадки в радиусе 10 км). Сеть должна содержать сайт (web-сервер) для проведения web-конференций.
19. Локальная сеть для подразделения издательской деятельности (Ventura, Page Maker, вёрстка, дизайн), базирующаяся на MAC-компьютерах.
20. Сеть для конструкторов КБ (конструкторского бюро) общего машиностроения.
21. Сеть для охраны небольшой фабрики: 4 web-камеры, мультимониторинг на каждом посту.
22. Бюджетная компьютерная сеть для средней школы, которая ищет спонсора. Один небольшой компьютерный класс на 15 машин. Компьютер у директора, в учительской и у преподавателя информатики.
23. Компьютерная сеть для средней школы с богатым спонсором. Два роскошных компьютерных класса на 15 машин каждый. Компьютер у директора, в учительской, а кабинеты физики, химии, информатики и актовый зал дополнительно оснащены проекторами.
24. Сеть в студенческом общежитии, где проживают будущие программисты (и возможно хакеры) и специалисты по IT-технологиям.

2.8.3 Требования к отчёту

Отчёт по данной работе оформляется в электронном виде в любой офисной системе, можно в виде презентации. Отчёт должен содержать:

- постановку задачи;
- функциональную схему локальной вычислительной сети;
- планирование структуры сети (описание сети, количество рабочих станций) ;
- способ управления сетью;
- план рабочих помещений;
- описание характеристик сервера (если он есть);
- архитектура сети (схема, описание);
- сетевые ресурсы;
- сетевые службы (обзор DHCP, DNS, WINS и их компоненты);
- организацию рабочего места;
- защиту информации в сети;
- приблизительные затраты на создание сети;
- заключение.

Отчёт не должен превышать 10–12 стандартных машинописных страниц формата А4. Присутствие цветных схем, диаграмм, картинок приветствуется.

2.9 Лабораторная работа. Модель взаимодействия открытых систем (OSI)

2.9.1 Требования к работе

Для проекта компьютерной сети, разработанной в лабораторной работе 2.8, построить 7-уровневую модель взаимодействия при выполнении сетевой работы. В эту модель необходимо включить:

- **Физический уровень**. Правильнее называть этот уровень механически-электрическим. Он включает в себя набор спецификации электрических и механических характеристик сетевого оборудования: напряжение, время сигнала, уровень данных, максимальная длина передачи и непосредственно физические устройства, а также обеспечивает передачу сигналов с помощью устройств с одного ПК на другой. На этом уровне живут типы проводов, типы разъёмов, уровни напряжения, сигналы модуляции.
- **Канальный уровень.** Обеспечивает функциональный и процедурный способы передачи данных между двумя устройствами, подключёнными к одной физической среде, фактически к одному кабелю. Пять основных функций, за которые отвечает канальный уровень: управление логической связью, осуществление сетевого доступа и обнаружение конфликтов, кадрирование данных, адресация, обнаружение ошибок.
- **Сетевой уровень.** Отвечает за передачу данных от одной конечной точки к другой, например, за передачу данных от ПК на сетевой концентратор, за передачу тех же данных на протяжении всего пути к другому ПК через маршрутизатор. Канальный уровень не умеет передавать информацию из одной такой сети в другую. Поэтому возникает необходимость в глобальном сетевом IP-адресе, который может быть присвоен каждому компьютеру в мировой сети независимо от того, как он связан с сетью – посредством модема, спутника или другого оборудования.
- **Транспортный уровень.** Основан на протоколе TCP/IP. Отвечает за доставку, исправление ошибок (запрос повтора передачи) при межсетевых обменах. Логическое подключение создаётся прежде, чем данные отправляются, и сохраняется в течение всего процесса передачи данных.
- **Сеансовый уровень.** Отвечает за управление сеансами между двумя взаимодействующими конечными точками, например за установление соединения между приложениями на сервере и клиенте. Сюда входит аутентификация, установка, прекращение и повторное соединение при необходимости.

- **Представительский уровень.** Является первым уровнем, связанным с передачей данных по сети на более абстрактном уровне, чем передача простых единиц и нулей. Уровень представления данных позволяет прочитать текст на машинах с разной кодировкой, распознать структуру каталогов на удалённой операционной системе.
- **Прикладной уровень.** На этом уровне выполняются приложения в сети. Используют специализированные протоколы каждой службы. Например: HTTP – для загрузки страничек web-браузерами; FTP – для удалённого взаимодействия с файловой системой; SMTP и POP3 – для отправки и получения почты; Telnet – для получения доступа к командной строке удалённого сервера. В сетях TCP/IP прикладные протоколы включают в себя функции представительского и сеансового уровней. Поэтому в сети TCP/IP все три уровня – прикладной, представительский и сеансовый – объединяют в один и называют прикладным.

2.9.2 Варианты заданий

Варианты заданий приведены в лабораторной работе 2.8.

Заключение

Несколько слов в завершение. Авторы в своей работе коснулись некоторых проблем создания, работы и настройки компьютерных сетей. В намерение авторов не входила попытка написать полновесный учебник по компьютерным сетям. Во-первых, имеется достаточное количество таких учебников, часть из них приведена здесь в списке литературы. Во-вторых, цель этого пособия несколько другая.
Авторы хотели бы донести до читателя понятие сложности компьютерных сетей, которая не является результатом лени и нерадивости сетевых инженеров. Компьютерные сети сложны изначально, потому что объединяют в своём составе самую разнообразную аппаратуру, которая управляется самыми разнообразными операционными системами, программами и драйверами.

Для управления такой сложной гетерогенной средой потребовался очень громоздкий многоуровневый стек протоколов TCP/IP, понять работу которого далеко не просто. Вот почему одной из целей авторов является поэтапное обучение читателей обращению с компьютерной сетью, чтобы не сеть управляла пользователем, а пользователь был в состоянии сделать сеть работоспособной.

Авторы далеки от мысли дать читателям универсальный метод, универсальный рецепт настройки сети, потому что такого метода не существует, как и не существует автоматизированных систем настройки сети. Практически всё приходится делать руками сетевого администратора.

Но авторы предполагают и надеются, что вдумчивый читатель, проработав все предложенные задания, не растеряется, оставшись наедине с компьютерной сетью, сможет сделать необходимые настройки и привести сеть в работоспособное состояние.
Изложены основные подходы. Настройка сети – задача комплексная, решать которую необходимо тоже комплексно. Приведены простейшие консольные команды для диагностики и наладки сети, а также поясняется их работа.

Рассмотрены простейшие программные средства для выяснения и изменения конфигурационных параметров локального компьютера: его MAC-адрес и IP-адрес. Показана настройка службы Proxy и трансляции сетевых адресов.

Предложен метод по определению «наружного» IP-адреса, номера AS (Autonomous System), текущего поставщика интернет-услуг. Показана возможность проверки проложенной маршрутизаторами трассы следования пакетов с использованием команд операционной системы.

Изложенные методы по возможности показаны в операционных системах Linux и MS Windows.

Старательному читателю, проработавшему все задания, в качестве самостоятельной работы предлагается несколько вариантов построения небольшой компьютерной сети.

Нельзя забывать, что огромная информационная система, называемая «глобальная компьютерная сеть», состоит из самых разнообразных компьютеров, включает самое разнообразное оборудование, сочленённое между собой тысячами проводов и связей, и, казалось бы, порвавши один из проводочков сеть должна бы «рухнуть», но она почему-то работает. Давайте ещё раз восхитимся работой этой новой технологии, которая теперь присутствует в нашей повседневной жизни.

Успехов и удачи!

Список использованных источников

1. Вишневский, А. Сетевые технологии Windows 2000 / А. Вишневский. – СПб. : Питер, 2000. – 591 с.

2. Галлагер, Р. Теория информации и надёжная связь / Р. Галлагер. – М. : Советское радио, 1974. – 720 с.

3. Компьютерные сети. Информационная безопасность и сохранение информации / В. А. Ганжа [и др.]. – Минск : БГУИР, 2014. – 128 с.

4. Иртегов, Д. В. Введение в сетевые технологии / Д. В. Иртегов. – СПб. : БХВ–Петербург, 2004. – 560 с.

5. Олифер, В. Г. Компьютерные сети. Принципы технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2010. – 945 с.

6. Столингс, В. Компьютерные сети, протоколы и технологии Интернета / В. Столингс. – СПб. : БХВ–Петербург, 2005. – 832 с.

7. Томас, М. Структура и реализация сетей на основе протокола OSPF / М. Томас. – М. : Вильямс, 2004. – 816 с.

8. Хелд, Г. Технологии передачи данных / Г. Хелд. – СПб. : БХВ–Петербург, 2003. – 720 с.

9. Чеппел, Л. TCP/IP. Учебный курс / Л. Чеппел, Э. Титтел; пер. с англ. – СПб. : БХВ–Петербург, 2003. – 976 с.

Св. план 2015, поз. 31

Учебное издание

Ганжа Виктор Александрович
Шиманский Валерий Владимирович

КОМПЬЮТЕРНЫЕ СЕТИ. ВВЕДЕНИЕ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *М. А. Зайцева*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *Е. Д. Степусь*

Подписано в печать 19.11.2015. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Bookman».
Отпечатано на ризографе. Усл. печ. л. 9,18. Уч.-изд. л. 8,0. Тираж 100 экз. Заказ 2.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6