

26 October 2022

History cleared

9 January 2023

Артурия ПендрагонHackthissite.org

01:28

Hackaday.com тут должны быть туториалы по взлому

01:28

Hacker101.com

01:28

21 February 2023

Артурия Пендрагон<https://chat.openai.com/chat>

12:42

26 February 2023

Артурия Пендрагон<https://habr.com/ru/post/535918/>

19:07

4 March 2023

Артурия Пендрагон

Отмеченные крестиком (*) самопроверкались за ненадобностью	
Номер	Темы разработок
802.1	Общие практические и практикума ЛВС
802.2	Управление логическим каналом
802.3 *	Ethernet
802.4	Маркерная шина (одно время использовалась в промышленных сетях)
802.5	Маркерные колоды (бренд фирмы IBM в технологии ЛВС)
802.6	Двойная двухнаправленная шина (рамки региональных сетей)
802.7	Техническая консультативная группа по широкополосным технологиям
802.8	Техническая консультативная группа по оптоволоконным технологиям
802.9	Изокронные ЛВС (для промышленной реальной времени)
802.10	Барабанные ЛВС и защита информации
802.11	Беспроводные ЛВС
802.12	Прикреплены запросами (для AnyLAN фирмы Hewlett-Packard)
802.13	Счастливый номер. Почему-то его никто не выбрал
802.14	Кабельные модемы (рабочая группа расследовала: в области кабельных модемов ее операторы применяли консорциум)
802.15	Персональные сети (Bluetooth)
802.16	Широкополосные беспроводные ЛВС
802.17	Гибкая топология и пакетного коллизий
802.18	Радиорегулирование
802.19	Со существованием сетей
802.20	Локальный межлокационный беспроводной доступ (аналог 802.16e)
802.21	Персональные, не зависящие от срока передачи данных (для передачи данных между технологиями)
802.22	Местные беспроводные сети

18:04

Артурия Пендрагон

1.6. Стандартизация сетей 97					
Номер	Темы разработок	Степень	Префикс	Степень	Префикс
802.5	Маркерные колоды (бренд фирмы IBM в технологии ЛВС)	10 ⁻³	милли	10 ³	1000
802.6	Двойная двухнаправленная шина (рамки региональных сетей)	10 ⁻⁶	микро	10 ⁶	1 000 000
802.7	Техническая консультативная группа по широкополосным технологиям	10 ⁻⁹	нано	10 ⁹	1 000 000 000
802.8	Техническая консультативная группа по оптоволоконным технологиям	10 ⁻¹²	пико	10 ¹²	1 000 000 000 000
802.9	Изокронные ЛВС (для промышленной реальной времени)	10 ⁻¹⁵	фемто	10 ¹⁵	1 000 000 000 000 000
802.10	Барабанные ЛВС и защита информации	10 ⁻¹⁸	атто	10 ¹⁸	1 000 000 000 000 000 000
802.11	Беспроводные ЛВС	10 ⁻²¹	цецто	10 ²¹	1 000 000 000 000 000 000
802.12	Прикреплены запросами (для AnyLAN фирмы Hewlett-Packard)	10 ⁻²⁴	юкто	10 ²⁴	1 000 000 000 000 000 000 000

18:43

Артурия Пендрагон

Степень	В явном виде	Префикс	Степень	В явном виде	Префикс
10 ⁻³	0,001	милли	10 ³	1000	Кило
10 ⁻⁶	0,000001	микро	10 ⁶	1 000 000	Мега
10 ⁻⁹	0,000000001	нано	10 ⁹	1 000 000 000	Гига
10 ⁻¹²	0,000000000001	пико	10 ¹²	1 000 000 000 000	Тера
10 ⁻¹⁵	0,0000000000000001	фемто	10 ¹⁵	1 000 000 000 000 000	Пета
10 ⁻¹⁸	0,0000000000000000000001	атто	10 ¹⁸	1 000 000 000 000 000 000	Экза
10 ⁻²¹	0,000000000000000000000000000001	цецто	10 ²¹	1 000 000 000 000 000 000	Цетта
10 ⁻²⁴	0,0000000000000000000000000000000000000001	юкто	10 ²⁴	1 000 000 000 000 000 000 000	Йотта

Артурия Пендрагон

АП

Для инженера-электрика (аналоговая) полоса пропускания, как 23:26 уже говорилось выше, это значение в герцах, указывающее ширину диапазона частот. Для компьютерного специалиста (цифровая) полоса пропускания — это максимальная скорость данных в канале, то есть значение, измеряемое в битах в секунду. аналоговая (Гц) или цифровая (бит/с) полоса пропускания

<https://www.youtube.com/live/pcf7Xr-fLoc?feature=share> 23:39

5 March 2023

АП

Артурия Пендрагон

16:59

Ряд Тейлора: К примеру, мы хотим аппроксимировать функцию $\cos(x)$ в окрестности точки $x=0$. Ряд Тейлора для $\cos(x)$ в этой точке будет выглядеть так:

$$\cos(x) \approx 1 - x^2/2! + x^4/4! - x^6/6! + \dots$$

Мы можем остановиться на любом конечном члене этого ряда, чтобы получить аппроксимацию $\cos(x)$ с определенной точностью.

Например, если мы возьмем первые два члена ряда, мы получим:

$$\cos(x) \approx 1 - x^2/2!$$

Эта формула будет давать более точный результат при малых значениях x , но будет менее точной при больших значениях.

АП

Артурия Пендрагон

17:25

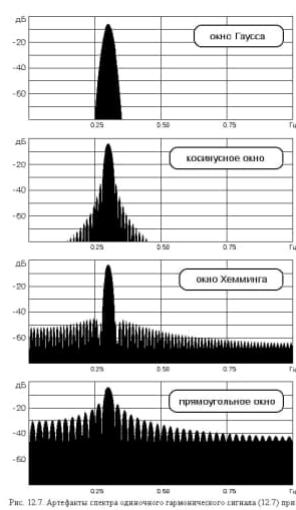


Рис. 12.7. Артефакты спектра одиночного гармонического сигнала (12.7) при использовании разных типов окна.

Прямоугольное окно:

в этом случае мы не изменяем сигнал и просто умножаем каждое значение на 1. Таким образом, результат останется без изменений.

Пример:

Вход: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

Выход: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

Окно Хемминга:

это окно, которое сглаживает края сигнала, чтобы избежать резких переходов и уменьшить артефакты. Пример:

Вход: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

Выход: [0.08, 0.21, 0.5, 0.79, 0.95, 0.95, 0.79, 0.5, 0.21, 0.08]

Косинусное окно:

это окно, которое уменьшает влияние краев сигнала и уменьшает артефакты. Пример:

Вход: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

Выход: [0.0, 0.15, 0.59, 1.0, 1.0, 0.59, 0.15, 0.0, 0.0, 0.0]

Окно Гаусса:

это окно, которое сглаживает сигнал и уменьшает артефакты, сохраняя при этом более высокие частоты, чем окна с большей длиной. Пример:

Вход: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

Выход: [0.05, 0.14, 0.38, 0.7, 0.93, 0.99, 0.93, 0.7, 0.38, 0.14]

Артурия Пендрогон

18:25

Амплитудный спектр и фазовый спектр – это две части спектра сигнала, которые описывают его свойства. Амплитудный спектр отражает амплитуду каждой частотной компоненты сигнала(Он представляет собой график, на котором по оси X откладываются частоты, а по оси Y – амплитуды.), а фазовый спектр – фазовый угол каждой компоненты(график, на котором по оси X откладываются частоты, а по оси Y – фазы).

Проще говоря, амплитудный спектр описывает, насколько громкими являются различные частоты в сигнале, а фазовый спектр описывает, как эти различные частоты настроены по времени.

Например, если мы говорим о звуке, то амплитудный спектр может показать, как сильно проявляется каждый инструмент в музыкальной композиции, а фазовый спектр может показать, насколько точно звучит каждая нота в музыке.

В целом, оба спектра являются важными инструментами для анализа сигналов и помогают понимать, как они устроены и как можно изменять их свойства.

6 March 2023

Артурия Пендрогон

23:21

Постулат теории информации гласит, что количество информации, которую можно передать, пропорционально количеству неопределенности в сообщении. Другими словами, чем более неопределенное сообщение, тем больше информации можно получить из него. Этот постулат был сформулирован Клодом Шенноном в 1948 году и стал основой для развития теории информации. Он является фундаментальным принципом для кодирования и передачи информации.

7 March 2023

Артурия Пендрогон

21:23

Бути відомим може мати різне значення для людей. Для деяких це матеріальне благополуччя, можливість долучатися до елітних подій та знайомств з відомими людьми. Інші бачать відомість як засіб для соціальної знаковості та впливу на громадські процеси. А деякі хочуть змінювати світ на краще. Але бути відомим має й недоліки. Публічні люди мають менше приватного життя та особистого простору. Їх можуть критикувати та насміхатися над ними. Вони

АП

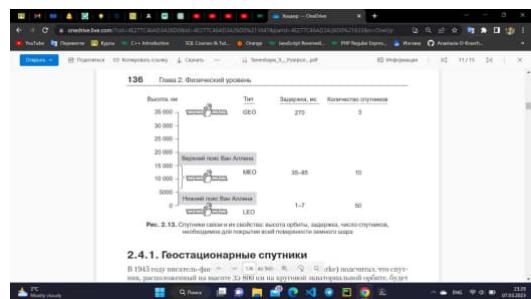
АП

АП

повинні стежити за своїми діями, оскільки це може вплинути на громадську думку та ставлення до них. Так що бути відомим має як переваги, так і недоліки.

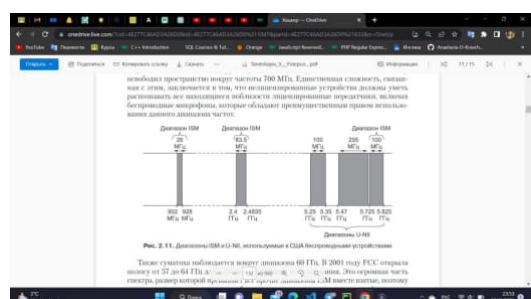
Артурия Пендрагон

23:29



Артурия Пендрагон

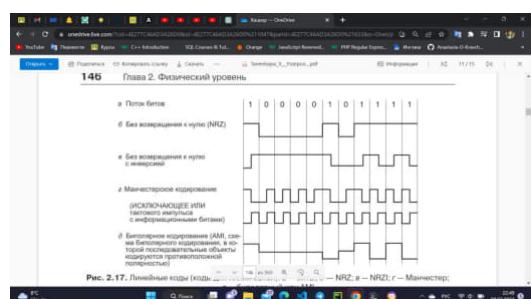
23:53



8 March 2023

Артурия Пендрагон

22:50



Артурия Пендрагон

23:24

Предположим, что у нас есть последовательность битов:
010110101011.

При использовании NRZI-кодирования с начальным уровнем "0", мы будем передавать сигнал в следующей последовательности:

Первый бит: 0 (начальный уровень) → не меняем уровень → сигнал на линии: 0

Второй бит: 1 → меняем уровень → сигнал на линии: 1

Третий бит: 0 → не меняем уровень → сигнал на линии: 1

Четвертый бит: 1 → меняем уровень → сигнал на линии: 0

Пятый бит: 1 → не меняем уровень → сигнал на линии: 0

Шестой бит: 0 → меняем уровень → сигнал на линии: 1

Седьмой бит: 1 → не меняем уровень → сигнал на линии: 1

Восьмой бит: 0 → меняем уровень → сигнал на линии: 0

Девятый бит: 1 → не меняем уровень → сигнал на линии: 0

Десятый бит: 0 → меняем уровень → сигнал на линии: 1

Одиннадцатый бит: 1 -> не меняем уровень -> сигнал на линии: 1
 Таким образом, мы получим сигнал на линии: 01100110110.

0 = 0 -> 1 = 0 -> 0 = 1 -> 010 ===> 001 23:30

Артурия Пендрагон 23:47

Допустим, у нас есть последовательность данных: 10101010. Мы хотим скремблировать эту последовательность, чтобы она выглядела более случайно и не имела длинных последовательностей нулей или единиц, которые могут вызвать проблемы при передаче данных.

Мы используем псевдослучайную последовательность в качестве маски для скремблирования нашей исходной последовательности данных. Например, пусть наша псевдослучайная последовательность будет 11001100.

Чтобы скремблировать нашу исходную последовательность, мы будем применять операцию "исключающее или" (XOR) между каждым битом нашей исходной последовательности и соответствующим битом псевдослучайной последовательности.

Таким образом, первый бит нашей исходной последовательности – 1 – будет скремблирован с первым битом псевдослучайной последовательности – 1 – по следующей формуле:

$$1 \text{ XOR } 1 = 0$$

Таким образом, первый бит нашей скремблированной последовательности будет равен 0.

Аналогично, второй бит нашей исходной последовательности – 0 – будет скремблирован с вторым битом псевдослучайной последовательности – 1 – по следующей формуле:

$$0 \text{ XOR } 1 = 1$$

Таким образом, второй бит нашей скремблированной последовательности будет равен 1.

Мы продолжим этот процесс для каждого бита в нашей исходной последовательности данных. После скремблирования нашей исходной последовательности данных с помощью псевдослучайной последовательности, получится новая, более случайная последовательность.

В нашем примере, после скремблирования исходной последовательности 10101010 с помощью псевдослучайной последовательности 11001100, мы получим следующую скремблированную последовательность: 01100110.

23:50

Данные (4B)	Ключевое слово (5B)	Данные (4B)	Ключевое слово (5B)
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

4B/5B – это метод кодирования, при котором каждые 4 бита данных кодируются в 5-битовый символ. Это позволяет улучшить надежность передачи данных за счет использования более сложной кодировки, которая обеспечивает более равномерное распределение нулей и единиц в передаваемых данных.

Например, чтобы закодировать последовательность из 8 бит (10101010), мы разбиваем ее на две группы по 4 бита: 1010 и 1010. Затем каждая группа кодируется в 5-битовый символ с помощью таблицы соответствий:

1010 – 11011
1010 – 11011

Таким образом, исходная последовательность 10101010 была закодирована в последовательность из двух 5-битовых символов 11011 11011.

Для декодирования мы просто применяем обратную операцию: разбиваем закодированную последовательность на группы по 5 бит и используем таблицу соответствий, чтобы преобразовать каждую группу в исходные 4 бита данных.

9 March 2023

Артурия Пендрагон

00:03

AMI (Alternate Mark Inversion) – это метод кодирования, который использует изменение полярности сигнала для кодирования цифр. Для этого используется три уровня напряжения: положительный (+), отрицательный (-) и нулевой (0).

Пример кодирования цифр с помощью AMI:

Цифра "1" кодируется с помощью полярности, то есть положительный и отрицательный уровни чередуются: +0-0+

Цифра "0" кодируется нулевым уровнем: 0000

Для синхронизации можно использовать специальный сигнал, например, последовательность "00000000".

Пример передачи сообщения "1010" с помощью AMI:

Цифра "1" кодируется с помощью полярности: +0-0+

Цифра "0" кодируется нулевым уровнем: 0000

Таким образом, сообщение "1010" будет закодировано в следующую последовательность: +0-0+0000+0-0+0000

Артурия Пендрагон

20:28

TDM Временное уплотнение можно сравнить с ситуацией, когда все пары людей говорят по очереди. **FDM** Частотное уплотнение мы

сравним с ситуацией, при которой люди говорят на разной высоте звука: одни на высокой, другие низкой, так что все ведут свои разговоры одновременно, но независимо от других. Для CDMA лучше всего подходит сравнение с ситуацией, когда все говорят одновременно, но каждая пара говорящих использует свой язык общения. Франкоговорящие промывают косточки всем остальным, воспринимая чужие разговоры как шум. Таким образом, ключевой идеей CDMA является выделение полезного сигнала при игнорировании всего остального

Артурия Пендрагон

23:07

Корреляция – это связь между двумя явлениями или наборами данных. Она показывает, насколько сильно два набора данных связаны между собой. Если корреляция *положительная*, то изменение одного набора данных сопровождается изменением другого набора данных в той же направленности. Если корреляция *отрицательная*, то изменение одного набора данных сопровождается изменением другого набора данных в противоположной направленности.

Ортогональность – это свойство, которое означает, что два объекта или вектора перпендикулярны друг другу, т.е. образуют прямой угол. В контексте математики, это означает, что две функции (или вектора) ортогональны, если их скалярное произведение равно нулю. Проще говоря, ортогональность означает, что два объекта *не пересекаются и не влияют друг на друга*.

Коды Уолша – это специальные последовательности, которые используются в технологии CDMA для передачи данных. Они состоят из множества элементов, которые могут быть либо "+1", либо "-1". Эти последовательности используются для кодирования и декодирования сигналов, чтобы каждый сигнал мог быть отделен от других и распознан как уникальный. Коды Уолша позволяют использовать общий диапазон частот для передачи нескольких сигналов одновременно, не мешая друг другу.

Артурия Пендрагон

23:45

В целом, телефонная система состоит из следующих трех главных компонентов.

1. **Местные линии связи** (аналоговые витые пары, подводящиеся в дома и офисы).
2. **Магистральные каналы** (цифровая связь на базе оптоволокна между коммутационными станциями).
3. **Коммутационные станции** (в них вызовы переадресуются с одних магистралей на другие).

10 March 2023

Артурия Пендрагон

08:49

Оксюморон – это сочетание двух слов, которые противоречат друг другу или кажутся несовместимыми. Например, "тихий крик", "честный вор", "горькая сладость", "живая мертвая".

Артурия Пендрагон

15:24

ограничение Шеннона говорит нам, что существует предельная скорость передачи информации, которую можно достичь через

канал связи без ошибок. Эта скорость зависит от ширины полосы канала и уровня шума, и если мы попытаемся передать информацию быстрее, чем это ограничение, то мы столкнемся с ошибками в передаче данных.

Артурия Пендрагон

21:39

PON – оптическая сеть с разделением сигнала и слиянием в один. Например, представьте, что есть оконечная станция, которая обслуживает 10 домов. Сигнал оптического интернета идет от станции к оптическому разделителю, который делит его на 10 частей – по одной для каждого дома. Каждый дом получает свою часть сигнала, и он используется для подключения к интернету. Когда информация отправляется из домов в интернет, оптические объединители собирают информацию из всех домов в единый поток, который отправляется обратно к оконечной станции.

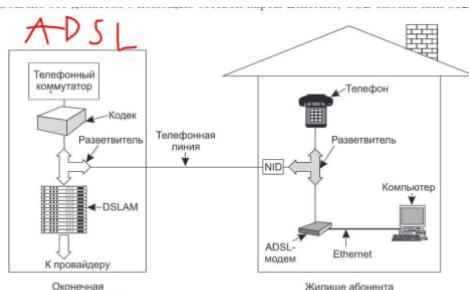


Рис. 2.31. Типичная конфигурация оборудования ADSL.



Рис. 2.32. Пассивная оптическая сеть для Волокна до дома

Артурия Пендрагон

21:42

ITU – занимается стандартизацией технологий связи, а также разработкой регуляторных и нормативных документов для телекоммуникационной отрасли.

Стандарт **SONET** и рекомендации **ITU** => **SDH** являются двумя основными стандартами для синхронной оптической сети. **SPE** = Кадры = способ передачи данных

Артурия Пендрагон

19:40

Главные цели при разработке системы **SONET** : 1)Обеспечение объединения сетей на разных носителях с помощью общего стандарта SONET.
2)Объединение цифровых систем США, Европы и Японии, построенных на 64 Кбит/с каналах.
3)Объединение нескольких цифровых каналов до скоростей, измеряемых в гигабитах в секунду.
4)Поддержка операций, администрирования и обслуживания (OAM).

T1 и **E1** – цифровые транспортные системы для передачи голоса и данных на скоростях 1,544 Мбит/с и 2,048 Мбит/с соответственно, использующие медные провода. T1 передает

данные по 24 каналам, E1 – по 32 каналам. Они обеспечивают синхронную передачу и используют метод PCM.

[Метод PCM](#) (Pulse Code Modulation) используется для преобразования аналоговых сигналов в цифровые. Он основан на том, что аналоговый сигнал дискретизуется с определенной частотой (обычно 8 кГц для голосовых сигналов) и каждое значение дискретизованного сигнала кодируется в цифровой код (обычно 8 или 16 бит).

Кодированный сигнал можно передавать по цифровым каналам связи, сохраняя при этом качество сигнала. На приемной стороне цифровой сигнал декодируется обратно в аналоговую форму, используя обратный метод PCM.

Артурия Пендрагон

21:01

[Оптоволоконные каналы](#) используют спектральное уплотнение ([WDM](#)), которое позволяет объединить несколько кабелей с разными частотами на одном волокне. Это осуществляется путем пропускания каждого сигнала через специальный фильтр, который пропускает только одну длину волн. Таким образом, каждый сигнал передается в своем частотном диапазоне, который успешно разделяется от других, что позволяет использовать один кабель для передачи нескольких сигналов. Таким образом, пропускная способность увеличивается линейно с числом каналов, и теоретически можно передавать большое количество данных на большие расстояния. Технология WDM развивается очень быстро и уже используется системы из 192 каналов по 10 Гбит/с и 64 каналов по 40 Гбит/с.

Интерферометры Фабри–Перо и Маха–Цандера – это приборы, которые используются для измерения длины световых волн и контроля спектрального состава света. Они состоят из двух зеркал, расположенных на небольшом расстоянии друг от друга, что создает интерференционную камеру, где свет отражается между зеркалами и создает интерференционную картину.

В [интерферометре Фабри–Перо](#) свет проникает в интерференционную камеру через полупрозрачный зеркальный зеркало и отражается от зеркала на обоих концах камеры. При определенных условиях на выходе из интерферометра можно получить яркие интерференционные полосы, которые используются для измерения длины волн.

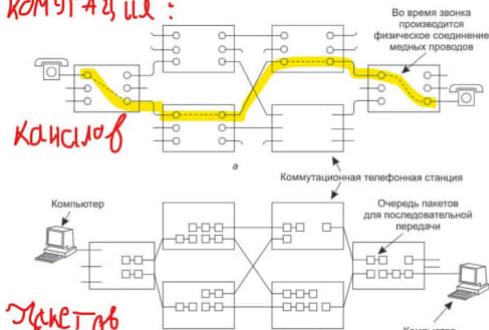
[Интерферометр Маха–Цандера](#) также использует два зеркала, но вместо того, чтобы пропускать свет через полупрозрачное зеркало, он использует два полностью отражающих зеркала. Входной свет проходит через полупрозрачную пластину, которая делит его на две части, и каждая из них отражается от зеркал и снова проходит через пластину, где они объединяются и создают интерференционную картину.

Интерферометры Фабри–Перо и Маха–Цандера используются в оптических системах, в том числе в WDM–системах, для настройки выходных фильтров на определенные частоты и обеспечения точного контроля спектрального состава света. Это позволяет создавать более гибкие оптические сети с множеством путей различной длины волны.



Артурия Пендрагон

КОММУТАЦИЯ:



Коммутация – Передача данных через сеть, позволяющая установить связь между отправителем и получателем.

Артурия Пендрагон

АП

Параметр	Коммутация каналов	Коммутация пакетов
Установка соединения	Требуется	Не требуется
Выделенный «медный» путь	Да	Нет
Каждый пакет перемещается по одному и тому же пути	Да	Нет
Пакеты приходят в правильном порядке	Да	Нет
Критичность выхода из строя коммутатора	Да	Нет
Доступная пропускная способность	Фиксированная	Динамическая
Возможность занятости линии	Во время установки соединения	Для каждого пакета
Возможность простых линий	Да	Нет
Передача с промежуточным хранением	Нет	Да
Оплата	За время на линии	За трафик

Коммутация каналов и **коммутация пакетов** отличаются тем, как передаются данные и как они оплачиваются.

1) При коммутации каналов передача данных осуществляется через выделенный канал связи, который оплачивается за время использования и расстояние передачи.

2) При коммутации пакетов данные разбиваются на пакеты и передаются через общий канал связи, который оплачивается за объем переданных данных.

Обычно телефонные сети используют коммутацию каналов для обеспечения хорошего качества звонка, а компьютерные сети используют коммутацию пакетов для простоты и эффективности. Но есть исключения, например, некоторые новые телефонные сети используют коммутацию пакетов для IP-телефонии, что позволяет сделать дешевые международные звонки, но может снизить качество звонка.

Мобил интернеинал:

- 1G: Аналоговая передача
- 2G: Цифровая передача
- 3G: Мобильный интернет
- 4G: Быстрый интернет
- 5G: Еще быстрее

Артурия Пендрагон

АП

Все 832 **канала** (это частотные диапазоны в радиоволновой системе связи, которые используются для передачи информации между отправителем и получателем) можно разделить на четыре категории.

1. **Управляющие** каналы (от базовой станции к мобильному телефону) для управления системой.
2. **Пейджинговые** каналы (от базовой станции к мобильному телефону) для передачи сообщений мобильным пользователям.
3. Каналы **доступа** (дву направленные) для установления соединения и назначения каналов.
4. Каналы **данных** (дву направленные) для передачи голоса, факса или данных.

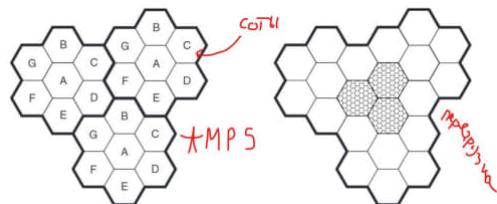
Для управления резервируется 21 канал. Поскольку одни и те же частоты не могут использоваться в соседних сотах, то число голосовых каналов, доступных в пределах одной ячейки, значительно меньше 832 — обычно около 45.

Коллизия — это конфликт между двумя или более устройствами, которые пытаются передать данные одновременно по одному и тому же каналу связи. 23:57

12 March 2023

Артурия Пендрагон

10:03

In reply to [this message](#)

AMPS (Advanced Mobile Phone System) — это стандарт первого поколения для цифровой сотовой связи, который был разработан в 1980-х годах.

AMPS использует аналоговую модуляцию и FDM (Frequency Division Multiplexing) для передачи голосовой информации. В AMPS каждый разговор использует свой уникальный канал, который разделен на два симметричных канала для передачи и приема. Система использует 832 дуплексных канала, каждый из которых состоит из пары симплексных каналов. Частоты этих каналов разделены между сотами и ячейками для минимизации коллизий.

AMPS также использует сигналы управления, такие как каналы доступа и каналы пейджинга для установления соединений и управления системой. В целом, AMPS предоставляет простую и надежную систему связи для передачи голоса, факса и данных, но по сравнению с более новыми цифровыми стандартами, такими как **GSM** и **CDMA**, имеет ограниченные возможности передачи данных и менее эффективное использование частотного спектра.

In reply to [this message](#)

10:06

Принцип работы: Это описание технологии мобильной связи AMPS, которая была изобретена компанией Bell Labs в 1982 году и использовалась в США, Англии и Японии. Система разбивала

географический регион на соты, которые работали на своих частотах и имели размеры от 10 до 20 км. Эта идея разбиения территории на ячейки давала AMPS большие возможности и более высокую производительность по сравнению с более ранними системами. В AMPS использовалась идея повторного использования частоты, что позволяло поддерживать несколько звонков на одной и той же частоте в удаленных друг от друга ячейках. При переполнении системы мощность передатчиков уменьшалась, а соты разбивались на микросоты. Это описание мобильной телефонной системы, в которой базовые станции соединены с коммутатором (MTSO/MSC), который связывается с телефонной сетью общего пользования через коммутацию пакетов. Мобильные телефоны находятся в зоне действия ячейки и управляются базовой станцией этой ячейки. Когда телефон покидает ячейку, его базовая станция опрашивает все окружающие станции и передает управление телефону ячейке, получающей от него наиболее сильный сигнал. Передача называется "handoff" и занимает около 300 мс. Базовые станции представляют собой радиоретрансляторы.

Артурия Пендрагон

10:56

АП



Рис. 2.40. Архитектура мобильной сети GSM

GSM – европейский стандарт мобильной связи второго поколения, который был впервые внедрен в 1991 году. Он основан на архитектуре, основанной на ячейках, что позволяет повторно использовать частоты и обеспечивает мобильность пользователей. Архитектура GSM аналогична архитектуре AMPS, но с разными названиями компонентов.

Артурия Пендрагон

14:05

АП

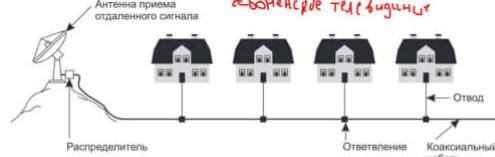


Рис. 2.44. Первая система кабельного телевидения

Артурия Пендрагон

19:28

АП

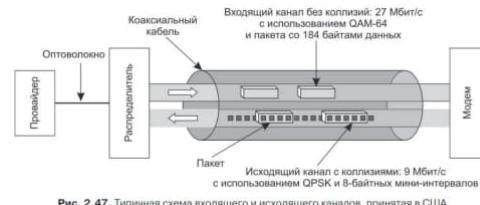


Рис. 2.47. Типичная схема входящего и исходящего каналов, принятая в США

13 March 2023

Артурия Пендрагон

17:19

Подсчет количества байтов – этот метод основывается на добавлении к кадру информации о его длине, чтобы получатель знал, сколько байтов ожидать. Пример: если кадр имеет длину 100 байтов, то

перед ним может быть добавлено 2 байта, содержащие значение 100.

Использование сигнальных байтов с символьным заполнением – этот метод заключается в добавлении специального символа (эскейп-символа) перед байтами, которые могут быть интерпретированы как сигнальные байты. Этот символ указывает на то, что следующий байт должен быть интерпретирован не как сигнальный байт, а как обычный байт. Пример: если в кадре присутствует байт-сигнал STX (стартовый символ текста) с кодом 0x02, то перед ним может быть добавлено эскейп-символ 0x1B, чтобы получатель мог правильно интерпретировать этот байт. ...данные... ESC 11111111 ESC ...данные...

Использование сигнальных битов с битовым заполнением – этот метод основывается на использовании специальных битовых последовательностей, которые указывают на начало и конец кадра. Пример: последовательность 01111110 может использоваться в качестве битового заполнения, а последовательность 01010101 может использоваться в качестве сигнальной последовательности.

Использование запрещенных сигналов физического уровня – этот метод заключается в использовании физически запрещенных сигналов, которые не могут появляться в данных. Это позволяет получателю определить начало и конец кадра. Пример: в Ethernet используется комбинация 8 байтов (10101010 10101010 10101010 10101010 10101010 10101010 10101011 10101011), которая не может появляться в данных, и поэтому может использоваться в качестве разделителя кадров.

Пreamble – это специальная последовательность бит, которая используется в начале передачи данных для синхронизации передающей и принимающей сторон.

Артурия Пендрагон

19:50

Поле – это множество элементов с заданными операциями сложения и умножения, удовлетворяющее определенным аксиомам.

Поле Q – поле рациональных чисел. Оно состоит из всех дробей вида a/b , где a и b являются целыми числами, $a \neq 0$. Примеры: $1/2, -3/4, 7/8$.

Поле R – поле действительных чисел. Оно состоит из всех чисел, которые можно представить на числовой оси. Примеры: 0, -1.5, 2.7.

Поле C – поле комплексных чисел. Оно состоит из всех чисел вида $a + bi$, где a и b являются действительными числами, i – мнимая единица ($i^2 = -1$). Примеры: $2 + 3i, -1 - 2i, 5i$.

Поле Z – кольцо целых чисел. Оно состоит из всех целых чисел (положительных, отрицательных и нуля). Примеры: -2, 0, 5.

Поле Q(e) – поле рациональных функций с коэффициентами в поле e (например, поле $Q(i)$, где i – мнимая единица). Оно состоит из всех выражений вида $P(x)/Q(x)$, где $P(x)$ и $Q(x)$ являются многочленами с коэффициентами в поле e , а $Q(x) \neq 0$. Примеры: $(2x + 1)/(x^2 - 1), (3i - 2)/(i^2 + 1), (5 + 2\sqrt{2}x)/(x^2 - 4)$.

Поле Галуа – поле с ограниченным числом элементов. Примером поля Галуа является поле $GF(2)$, которое состоит из двух элементов – 0 и 1. В этом поле операция сложения эквивалентна операции XOR (исключающее ИЛИ), а операция умножения эквивалентна операции AND (логическое И). Другой пример поля Галуа – поле $GF(7)$, которое состоит из семи элементов – 0, 1, 2, 3, 4, 5 и 6. В этом поле операции сложения и умножения выполняются по модулю 7. Например, $3 + 5 = 1$ (поскольку $8 = 1$ по модулю 7), а $2 * 4 = 1$ (поскольку $8 = 1$ по модулю 7).

Например, если мы используем поле Галуа $GF(2)$ (также известное как бинарное поле), то мы можем представлять числа только как 0 или 1. В этом случае операции сложения и умножения соответствуют операциям логического XOR и логического AND соответственно.

Например, $1 + 1 = 0$ (поскольку $1 \text{ XOR } 1 = 0$), а $1 * 1 = 1$ (поскольку $1 \text{ AND } 1 = 1$).

В этом поле мы можем использовать коды проверки четности, где мы добавляем дополнительный бит, который равен сумме всех битов сообщения по модулю 2 (т.е. XOR всех битов). Таким образом, мы можем обнаруживать ошибки, если какой-то из битов в сообщении был изменен.

<https://www.youtube.com/watch?v=ZIMekfvEd3I>

19:51

АП **Артурия Пендрагон**

23:06

сверточным кодом:

<https://youtu.be/hNXmeRlc94Q>

кодом Рида—Соломона:

<https://habr.com/ru/post/538870/>

15 March 2023

АП **Артурия Пендрагон**

19:37



Рис. 3.11. Скользящее окно размера 1 с 3-битовым передовыми номером: а — начальная ситуация; б — после отправки первого кадра; в — после приема первого кадра; г — после приема первого подтверждения

АП **Артурия Пендрагон**

23:10

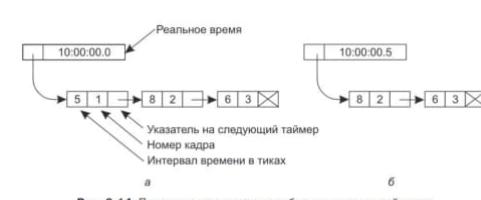


Рис. 3.14. Программная симуляция работы нескольких таймеров

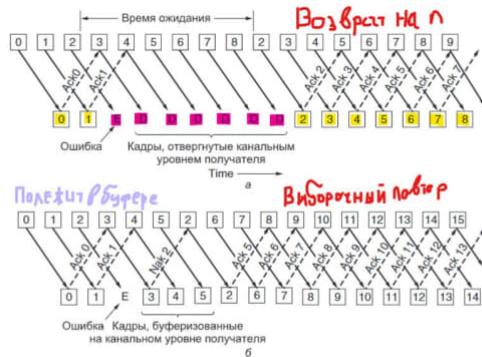


Рис. 3.13. Конвейеризация и коррекция ошибок: а — эффект при размере окна 1; б — эффект при размере окна больше 1.

16 March 2023

Артурия Пендрагон

18:03

RAW – без потерь

JPEG – сжатый формат

GIF – анимированный формат

PNG – формат с поддержкой прозрачности

TIFF – высококачественный формат

BMP – формат без сжатия

Артурия Пендрагон

22:26

PPP (Point-to-Point Protocol) – это протокол, используемый для передачи данных между двумя узлами сети через серийный (например, модемный) канал связи. Он позволяет установить соединение между двумя устройствами, произвести аутентификацию и обеспечить надежную передачу данных. Для пересылки пакетов по таким каналам.

17 March 2023

Артурия Пендрагон

11:43

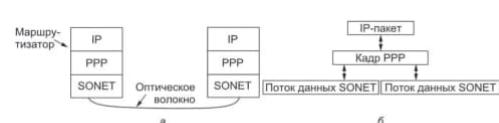


Рис. 3.16. Пакеты передаются по протоколу SONET: а — стек протоколов; б — взаимоотношение между кадрами.



Рис. 3.17. Полный формат кадра PPP для работы в ненумерованном режиме

11:48

Артурия Пендрагон

16:19

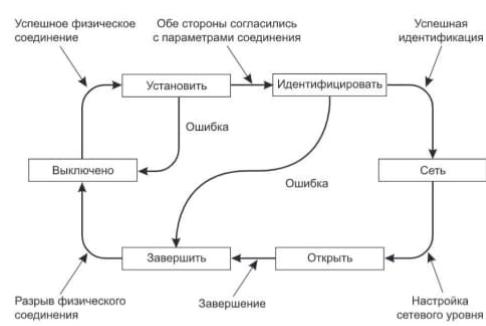


Рис. 3.18. Диаграмма состояний установки и разрыва соединения PPP

АП

17:18

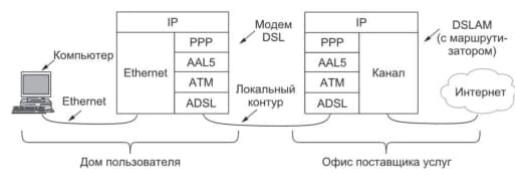
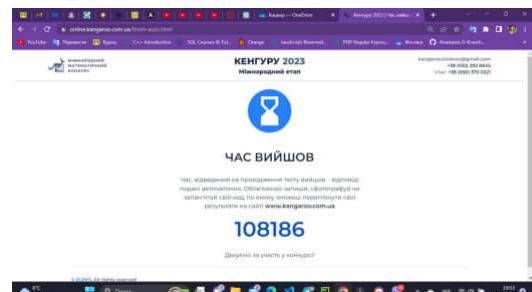
Артурия Пендрагон

Рис. 3.19. Стек протоколов ADSL

Артурия Пендрагон

19:03

**Артурия Пендрагон**

19:18

АП

Фрази для запам'ятовування:

- **Буде ГоЖе Гедзю у Джазі — дзвінкі** приголосні.
- **Усе Це Кафе «Птах і Чаша» — глухі** приголосні.
- **Ми Винили Рій — сонорні.**

Артурия Пендрагон

21:00

АП



Рис. 3.20. Кадр AAL5, содержащий данные PPP

18 March 2023

Артурия Пендрагон

16:44

<https://habr.com/ru/company/nerepetitor/blog/253755/>**Артурия Пендрагон**

18:54

АП

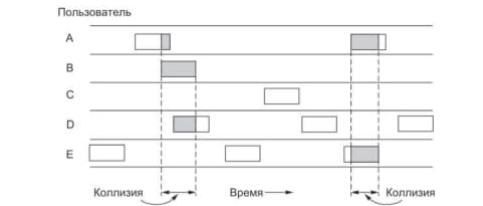


Рис. 4.1. В чистой системе ALOHA кадры передаются в абсолютно произвольное время

Артурия Пендрагон

19:48

АП

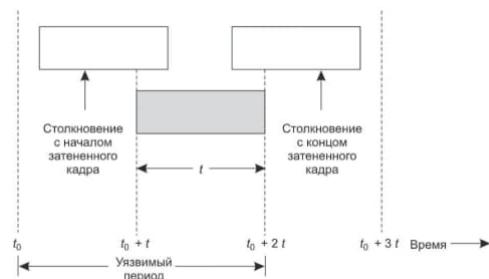


Рис. 4.2. Уязвимый период времени для затененного кадра

АП

Артурия Пендрагон

21:47



Рис. 4.5. Протокол CSMA/CD может находиться в одном из трех состояний: конкуренции, передачи и простое

19 March 2023

АП

Артурия Пендрагон

12:46



Протокол битовой карты – это способ передачи информации между устройствами, который основывается на использовании битовых карт.

Передача информации осуществляется путем передачи битовой карты от одного устройства к другому, где каждый бит представляет определенное устройство или данные. Получив битовую карту, устройство может интерпретировать информацию о статусе устройств и принять соответствующие действия.

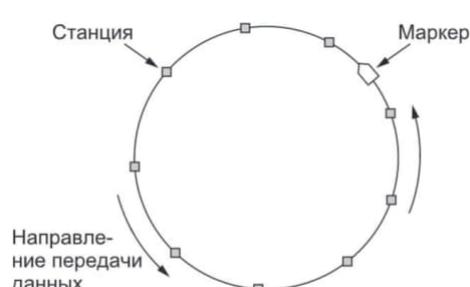


Рис. 4.7. Маркерное кольцо

12:55

В компьютерных сетях **маркер** – это символ или бит, который передается от узла к узлу для контроля доступа к разделяемому каналу связи. Узел, который получает маркер, имеет право передавать данные по каналу. Когда передача данных завершается, узел передает маркер следующему узлу в сети. Этот процесс повторяется, пока все узлы не получат возможность передавать данные.

Правило арбитража – это механизм разрешения споров между двумя или более сторонами путем урегулирования их разногласий третьей независимой стороной – арбитром или арбитражным судом.

13:03



Рис. 4.8. Протокол с двоичным обратным отсчетом. Прочерк означает молчание

Двоичный обратный отсчет – это метод, который используется для синхронизации сигналов в цифровых сетях. Он работает путем отсчета сигналов в обратном порядке от заранее определенного значения до нуля. Каждый отсчет в обратном отсчете представлен в двоичной форме, где каждая цифра (0 или 1) соответствует состоянию сигнала на определенном моменте времени. Этот метод позволяет установить точный момент начала передачи данных, так как все устройства в сети синхронизируются с одним общим отсчетом.

Артурия Пендрагон

13:58

дискретность = квантование(Интервальность)

Асимметричный = неравный

Дифференция = дискретная разность(Изменение)

Асимптотический = приближенный

асимптотический = Бесконечносый

Интерференция = Взаимодействие

Артурия Пендрагон

14:38

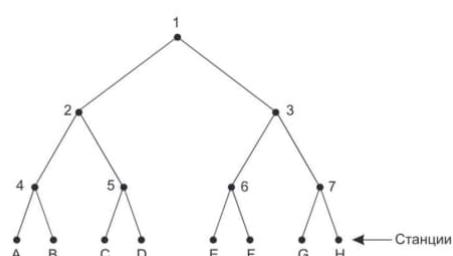


Рис. 4.10. Дерево из восьми станций

во время Второй мировой войны в армии США для проверки солдат на сифилис (Dorfman, 1943). Брался анализ крови у N солдат. Часть каждого образца помещалась в одну общую пробирку. Этот смешанный образец проверялся на наличие антител. Если антитела не обнаруживались, все солдаты в данной группе объявлялись здоровыми. В противном же случае группа делилась пополам, и каждая половина группы проверялась отдельно. Подобный процесс продолжался до тех пор, пока размер группы не уменьшался до одного солдата.

Артурия Пендрагон

15:50

In reply to [this message](#)

$2^{i-1} \rightarrow$ Сколько станций могут быть определены для передачи;

$2^{i-1}q \rightarrow q$ – количество готовых станций,

$i = \log_2 q$

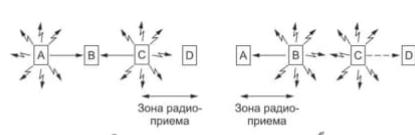
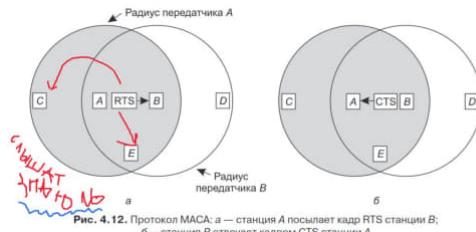


Рис. 4.11. Беспроводная локальная сеть: а — А и С — скрытые станции во время пересылки данных на В; б — В и С — засвеченные станции во время пересылки данных на А и D

15:50

проблемы, которые могут возникать при передаче данных в беспроводной сети между несколькими станциями, когда одна станция не может слышать другую станцию, находящуюся слишком далеко от нее. Это приводит к возникновению двух типов проблем: проблемы скрытой станции, когда одна станция не слышит конкурента, и проблемы засвеченной станции, когда станция ошибочно предполагает, что не может передавать данные из-за выполняющейся передачи другой станции. Для решения этих проблем используется MAC-протокол, который предотвращает коллизии и задержки в передаче данных между станциями.



15:55

MACA (Multiple Access with Collision Avoidance— множественный доступ с предотвращением коллизий) (Karn, 1990). Идея, лежащая в основе этого протокола, заключается в том, что отправитель заставляет получателя передать короткий кадр, чтобы окружающие станции могли услышать эту передачу и воздержаться от действий на время, требуемое для приема большого информационного кадра. Эта техника заменяет технику прослушивания несущей.

RTS – запрос на передачу

CTS – разрешение передачи

персональных (**PAN**), локальных (**LAN**) и общегородских (**MAN**) 16:03 сетей стандартизировано в серии стандартов IEEE 802

Основные выводы, которые можно сделать после прочтения 16:17 книги Чарльза Дарвина "Происхождение видов":

Виды не были созданы независимо, а эволюционировали из простейших форм жизни.

Естественный отбор – это процесс, который позволяет выживать наиболее приспособленным организмам в конкретной среде.

Переменчивость наследственности является ключевой составляющей эволюции, так как она обеспечивает разнообразие в популяции и возможность адаптации к изменяющимся условиям среды.

Возникновение новых видов происходит благодаря накоплению мелких изменений в популяции на протяжении многих поколений. Эволюция – это процесс, который продолжается и по сей день, и человек является результатом этого процесса.

Концепция Дарвина вызвала много споров и дискуссий, но в настоящее время она широко признана и подтверждена многими исследованиями в различных областях науки.

Концепция Дарвина:

Принцип естественного отбора.

Происхождение видов путем естественного отбора.

Разнообразие видов и их адаптация к среде обитания.

Отсутствие постоянства видов.

Эволюционное развитие происходит постепенно и непрерывно.

Общее происхождение разных видов живых организмов.

Единство жизни на Земле.

Важность генетического наследования и мутаций в эволюционном процессе.

Конкуренция и борьба за выживание в природе.

Существует два типа Ethernet: **классический Ethernet** (classic Ethernet), который решает проблему множественного доступа с помощью техник, представленных в этой главе; и **коммутируемый Ethernet** (switched Ethernet), в котором для соединения компьютеров используются устройства под названием коммутаторы.

Боб Меткальф + Дэвидом Боггсом + исследовательский центр Xerox => Ethernet в честь люминофорного эфира, через который, как когда-то считалось, распространяются электромагнитные лучи

Артурия Пендрагон

19:20

Опыт Майкельсона–Морли был проведен в 1887 году и имел целью проверить гипотезу о стационарности эфира, предполагавшую, что свет распространяется в эфире, который является абсолютным пространством.

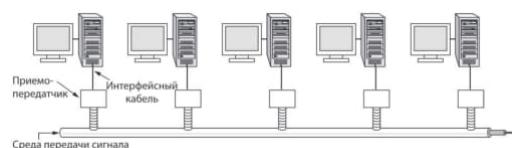
Основные выводы, которые были сделаны после проведения опыта, можно пронумеровать следующим образом:

Опыт не выявил никакой зависимости скорости света от скорости движения Земли вокруг Солнца.

Это противоречило гипотезе о стационарности эфира и подтверждало теорию относительности Эйнштейна, которая утверждает, что скорость света не зависит от движения источника света и наблюдателя.

Опыт стал одним из самых известных и значимых в истории науки, поскольку он дал решающий толчок для развития новой теории относительности и отверг гипотезу о стационарности эфира.

Опыт Майкельсона–Морли стал отправной точкой для многих других экспериментов, направленных на изучение свойств света и понимание его природы.



19:27

Рис. 4.13. Архитектура классической сети Ethernet

Толстый/Тонкий изирнет 500/135 м 100/30 шт

Артурия Пендрагон

19:57

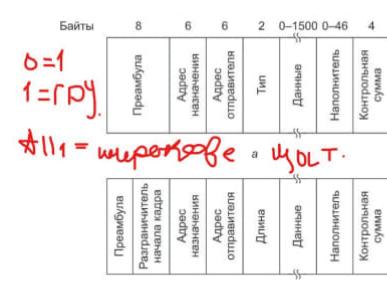


Рис. 4.14. Форматы кадров: а — DIX Ethernet; б — IEEE 802.3

АП

Артурия Пендрагон

20:41

экспонента = е

20 March 2023

Артурия Пендрагон

15:58

АП

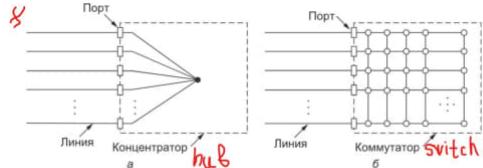


Рис. 4.17. Конфигурация Ethernet: а — концентратор; б — коммутатор

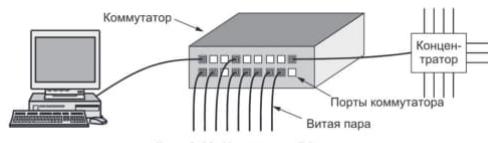


Рис. 4.18. Коммутатор Ethernet

16:02

стандартными разъемами RJ-45 для подключения витой пары.

Каждый кабель соединяет коммутатор или концентратор с одним компьютером

Артурия Пендрагон

16:37

АП

В качестве одного из следствий закона Паркинсона («Работа занимает все отведенное на нее время») можно привести следующее правило: «Данные занимают всю предоставленную пропускную способность канала». (Согласно закону Паркинсона, "работа расширяется так, чтобы заполнить доступное время для ее выполнения". Иными словами, чем больше времени мы выделяем на выполнение задачи, тем больше времени мы на нее потратим, даже если эта задача может быть выполнена за меньшее время.)

Fast Ethernet => 802.3u

16:43

Жаргонизмы (жаргонная лексика) – это слова, употребление которых свойственно людям, образующим обособленные социальные группы

Артурия Пендрагон

18:19

АП

"Моноканалы" – это вероятно отсылка к аудио-интерфейсам, где используются разъемы типа "моно джек" или "стерео джек" для подключения одного или двух каналов звука соответственно.

"Ответвители типа 'зуб вампира'" могут относиться к специализированным разъемам, используемым в электронике или электрике для подключения нескольких проводов или кабелей в один разъем.

"BNC-коннекторы" – это разъемы, используемые в сферах связи и видео для передачи сигналов высокой частоты и/или сигналов со временным кодом.

Артурия Пендрагон

19:48

АП

Таблица 4.2. Основные типы кабелей для сетей Fast Ethernet

Название	Тип	Длина сегмента, м	Преимущества
100Base-T4	Витая пара	100	Использование незакранированной витой пары категории 3
100Base-TX	Витая пара	100	Полный дуплекс при 100 Мбит/с (витая пара 5 категорий)
100Base-FX	Оптоволокно	2000	Полный дуплекс при 100 Мбит/с; большая длина сегмента

АП

Артурия Пендрагон

Gigabit Ethernet => 802.3ab

20:29

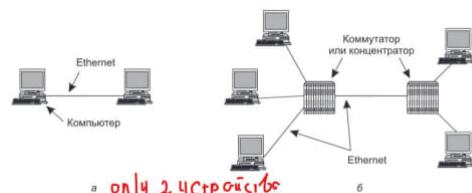


Рис. 4.19. Сеть Ethernet, состоящая: а – из двух станций; б – из множества станций

АП

Артурия Пендрагон

21:15

Таблица 4.3. Кабели Gigabit Ethernet

Название	Тип	Длина сегмента, м	Преимущества
1000Base-SX	Оптоволокно	550	Многомодовое волокно (50, 62,5 мкм)
1000Base-LX	Оптоволокно	5000	Одномодовое (10 мкм) или многомодовое (50, 62,5 мкм) волокно
1000Base-CX	2 экранированные витые пары	25	Экранированная витая пара
1000Base-T	4 незакранированные витые пары	100	Стандартная витая пара 5-й категории

АП

Артурия Пендрагон

21:51

PAUSE — это, на самом деле, обычные кадры Ethernet, в поле Type которых записано 0x8808. Продолжительность паузы определяется в единицах времени передачи минимального кадра. Для Gigabit Ethernet такая единица равна 512 нс, а паузы могут длиться до 33,6 мс.

Таблица 4.4. Кабели 10-Gigabit Ethernet

Название	Тип	Длина сегмента	Преимущества
10GBase-SR	Оптоволокно	До 300 м	Многомодовое волокно (0,85 мкм)
10GBase-LR	Оптоволокно	10 км	Одномодовое (1,3 мкм) волокно
10GBase-ER	Оптоволокно	40 км	Одномодовое (1,5 мкм) волокно
10GBase-CX4	4 пары биаксиального кабеля	15 м	Биаксиальный медный кабель
10GBase-T	4 пары незакранированной витой пары	100 м	Незакранированная витая пара категории 6a

БПД— будь проще, дурачок (KISS — KeepItSimple,Stupid)

21:58

21 March 2023

АП

Артурия Пендрагон

15:30

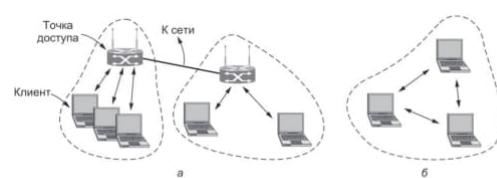


Рис. 4.20. Архитектура сети стандарта 802.11: а — инфраструктурный режим; б — произвольный режим

инфраструктурном режиме => связывают режимами точкой доступа (Access Point, AP) => соединяют в кабельную сеть распределительная система

произвольной сетью

15:34



Рис. 4.21. Часть стека протоколов 802.11

Что касается 802.11, то подуровень MAC (подуровень управления доступом к среде) отвечает за распределение канала, то есть за то, какая станция будет передавать следующей. Над MAC в иерархии находится подуровень LLC (управления логическим соединением), задача которого состоит в том, чтобы сделать различия стандартов 802.x невидимыми для сетевого уровня. Это могло бы стать очень ответственной задачей, но в настоящее время ключевым слоем считается LLC; именно он отвечает за идентификацию про-токола (например, IP), информация о котором передается в кадре 802.11.

первоначальные методами передачи:
инфракрасная передача
скаккообразного изменения частоты в диапазоне 2,4ГГц
широкополосный сигнал с прямой последовательностью ==
802.11b.

15:37

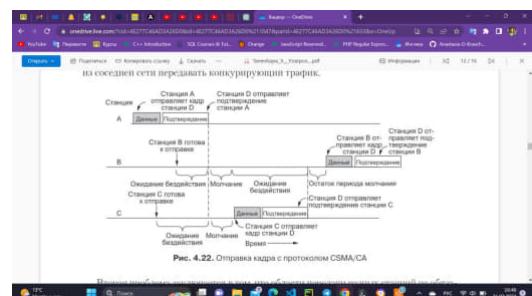
Артурия Пендрагон

16:38

Стандарт	Применение	Скорость	Частотный диапазон	Расширение спектра	MIMO	Совместимость
802.11a	Высокоскоростная беспроводная передача данных	54 Мбит/с	5 ГГц	OFDM	Нет	Несколько
802.11b	Домашняя и офисная беспроводная сеть	11 Мбит/с	2,4 ГГц	DSSS	Нет	Высокая
802.11g	Улучшение стандарта 802.11b с более высокой скоростью передачи данных и обратной совместимостью	54 Мбит/с	2,4 ГГц	DSSS, OFDM	Нет	Высокая
802.11n	Беспроводная передача данных с высокой скоростью и дальностью при использовании MIMO	До 600 Мбит/с	2,4 ГГц и/или 5 ГГц	OFDM, MIMO	Да	Обратная совместимость с 802.11a/b/g

802.11a/b/g/n

16:46



Артурия Пендрагон

17:36

DCF – это метод, который используется в большинстве беспроводных сетей Wi-Fi, который основан на CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) и использует случайное ожидание передачи данных. Когда устройство готово отправить данные, оно прослушивает среду на наличие других передач. Если среда свободна, устройство начинает передавать данные. Если же среда занята, устройство ждет случайное время и повторяет попытку передачи.

PCF (Point Coordination Function) – это один из двух методов доступа к среде (MAC-протоколов), используемых в стандарте беспроводной сети Wi-Fi 802.11. PCF является дополнительным методом, который используется вместе с основным методом доступа к среде – DCF (Distributed Coordination Function).

PCF позволяет точке доступа (AP) управлять передачей данных между устройствами в беспроводной сети. В режиме PCF, точка доступа принимает на себя роль "координатора" и регулирует передачу данных между устройствами. Точка доступа контролирует доступ к среде и разрешает устройствам передавать данные только тогда, когда она разрешает.

Режим PCF используется редко в современных беспроводных сетях, так как DCF обеспечивает более гибкий и эффективный способ доступа к среде. Однако, в некоторых сценариях, например, в сетях с высокой плотностью устройств, PCF может быть полезен для управления передачей данных и улучшения качества обслуживания.

Артурия Пендрагон

18:37

АП



Рис. 4.24. Использование прослушивания виртуального канала в протоколе CSMA/CA

Артурия Пендрагон

19:45

АП



Рис. 4.25. Межкадровые интервалы в стандарте 802.11

Для беспроводных сетей стандарта 802.11 существуют различные временные интервалы, такие как DIFS, SIFS, AIFS и EIFS. DIFS используется для определения возможности захвата канала, SIFS используется для передачи приоритетных кадров, AIFS используется для задания приоритетов передачи кадров различных уровней, а EIFS используется для обнаружения испорченных кадров. Расширения стандарта включают понятие возможности передачи (TXOP), которое позволяет станциям отправлять несколько кадров за один раз и улучшает качество обслуживания.

аномалия скорости – ситуация, когда скорость передачи данных на компьютере или в сети не соответствует ожидаемой скорости или колеблется в большой диапазон. 19:50

Артурия Пендрагон

20:11

АП



Рис. 4.26. Информационный кадр стандарта 802.11

Артурия Пендрагон

АП

Стандарт 802.11 определяет сервисы для беспроводных ЛВС. 20:40

Сервисы можно разделить на категории: ассоциация, реассоциация, дизассоциация, аутентификация.

Ассоциация используется для подключения мобильных станций к точкам доступа и узнавания их возможностей.

Реассоциация позволяет станции сменить точку доступа.

Дизассоциация используется для разрыва отношений между станцией и точкой доступа.

Аутентификация требуется для отправки кадров через точку доступа.

Рекомендуемая схема безопасности называется **WPA2** и обеспечивает безопасность, как определено стандартом 802.11i. Схема, используемая до WPA, называется **WEP**. Аутентификация с предустановленным ключом выполняется перед ассоциацией. Ее польза не велика из-за недостатков конструкции, делающих WEP легко взламываемым.

Кадры, достигающие точки доступа, определяются службой **распределения** (distribution service), которая определяет их маршрутизацию. Если адрес назначения является локальным для данной точки доступа, то кадры следуют напрямую по радиоканалу. В противном случае, их необходимо пересыпать по проводной сети. Служба **интеграции** (integration service) поддерживает трансляцию, необходимую, если кадр нужно выслать за пределы сети стандарта 802.11 или если он получен из сети не этого стандарта. Типичный случай здесь — соединение между беспроводной ЛВС и Интернетом. Служба **доставки данных** (data delivery) является ключевой в работе сети, так как сеть 802.11 существует для обмена данными. Эта служба позволяет станциям передавать и получать данные по протоколам, которые описаны ранее. Стандарт 802.11 основан на стандарте Ethernet, где доставка данных не является гарантированной на 100%, поэтому для беспроводных сетей это тем более верно. Верхние уровни должны заниматься обнаружением и исправлением ошибок.

Служба **конфиденциальности** (privacy service) отвечает за зашифрование информации, посланной по беспроводной ЛВС, для сохранения ее конфиденциальности. Алгоритм шифрования для WPA2 основан на AES, американском правительственный стандарте, одобренном в 2002 году. Ключи, используемые для шифрования, определяются во время процедуры аутентификации.

Служба **планирования трафика QOS** (QOSScheduling) обрабатывает трафик с различными приоритетами и использует протоколы, чтобы дать голосовому и видео трафику преимущество перед трафиком «с максимальными усилиями» и фоновым трафиком.

Есть две службы, которые помогают станциям управлять использованием спектра.

Регулирование мощности передатчика дает информацию, необходимую для соответствия установленным нормам мощности передачи.

Служба **динамического выбора частоты** предотвращает передачу в частотном диапазоне, используемом радарами.

Стандарт 802.11 обеспечивает возможности для соединения мобильных клиентов с Интернетом.

Стандарт неоднократно исправлялся, чтобы добавить еще больше возможностей.

Артурия Пендрагон

АП

16:56



Рис. 4.27. Архитектура стандарта 802.16



Рис. 4.28. Стек протоколов 802.16

Артурия Пендрагон

АП

17:19

OFDM (ортогональное частотное разделение каналов) – это метод модуляции сигнала, используемый в цифровых системах связи. Он позволяет передавать данные в различные поднесущие, которые являются ортогональными друг другу, что снижает межсимвольные помехи и повышает эффективность передачи данных.

Артурия Пендрагон

АП

17:37

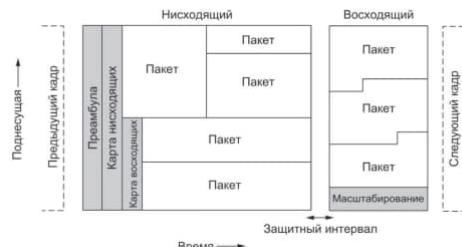


Рис. 4.29. Структура кадра для OFDMA и дуплекса с временным разделением

TDD (Time Division Duplex— дуплекс с временным разделением)

FDD (Frequency Division Duplex)

Деградация сигнала – это потеря качества или ухудшение сигнала при передаче, обработке или хранении информации.

масштабирования (ranging) — это процесс, при котором новые станции корректируют свою синхронизацию и запрашивают начальную полосу пропускания, чтобы соединиться с базовой станцией.

Артурия Пендрагон

АП

19:15



Рис. 4.30. Кадр: а — обычный; б — запроса канала

Бит ЕС говорит о том, шифруется ли поле данных. Поле Тип указывает тип кадра (в частности, сообщает о том, пакуется ли кадр и есть ли фрагментация). Поле СI указывает на наличие либо отсутствие поля финальной контрольной суммы. Поле ЕК сообщает,

какой из ключей шифрования используется (если он вообще используется). В поле Длина содержится информация о полной длине кадра, включая заголовок. Идентификатор соединения сообщает, какому из соединений принадлежит кадр. В конце заголовка имеется поле Контрольная сумма заголовка, значение которого вычисляется с помощью полинома $x^8 + x^2 + x + 1$

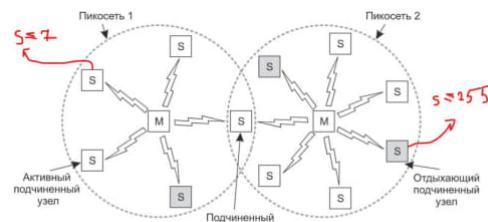
Артурия Пендрагон

19:56

АП Полином – это выражение, состоящее из суммы или разности произведений различных переменных и констант, возвещенных в различные степени. Например, полиномом может быть выражение $x^2 + 3x - 2$.

Bluetooth («Синий зуб») в честь великого короля викингов по 20:04 имени Гаральд Синий Зуб II (940—981), который объединил, (читай, завоевал) Данию и Норвегию. Ну да, он тоже сделал это без помощи проводов.

Консорциум – это объединение нескольких организаций или 20:16 компаний с целью совместной работы над определенным проектом или достижением определенной цели.



20:23

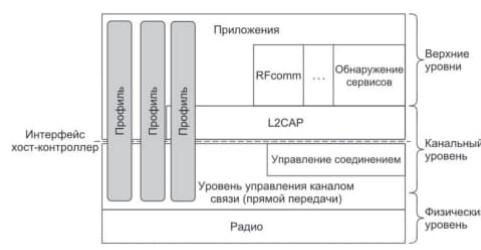
Рис. 4.31. Две пикосети могут, соединившись, сформировать рассеянную сеть

Артурия Пендрагон

21:00

АП Профили=приложения со своими протоколами => intercom телефонный конект; HID человеческий конект(соединения с компьютером клавиатур и мышей)

В апреле 1968 года в журнале Datamation была опубликована 21:01 статья Мелвина Конвея (Melvin Conway), в которой он высказал идею, что структура программного обеспечения отражает структуру группы разработчиков. Он утверждал, что если поручить написание компилятора n программистам, то получится n-проходный компилятор. То есть, каждый программист, скорее всего, напишет отдельный модуль компилятора, который будет иметь свою специфическую функцию. В результате получится более сложная структура программного обеспечения, чем если бы компилятор писал один программист. Это наблюдение получило название "Закон Конвея".



21:07

Синий зуб Протокол канального уровня— это L2CAP (протокол 21:19 управления логическими каналами и согласования). Он собирает

сообщения переменной длины и при необходимости обеспечивает надежность.

"Эмулировать" означает создать программную или аппаратную среду, которая имитирует поведение другой среды или устройства. Например, компьютерная программа может эмулировать работу старой игровой консоли, чтобы игроки могли играть в старые игры на современных компьютерах.

Артурия Пендрагон

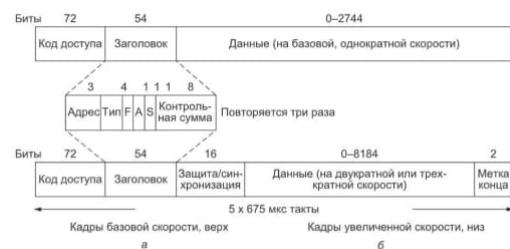
21:54

Соединения: SCO синхронный с установлением связи(наушники); ACL асинхронный без установления связи(коммутация пакетов)PS максимум усилий

Протокол RFcomm эмулирует работу стандартного последовательного порта ПК, к которому обычно подключаются клавиатура, мышь, модем и другие устройства.

Протокол канального уровня — это L2CAP (Logical Link Control and Adaptation Protocol — протокол управления логическими каналами и согласования). Он собирает сообщения переменной длины и при необходимости обеспечивает надежность.

"Такт" в технологии Bluetooth — это единица измерения времени, которая используется для синхронизации передачи данных между устройствами, соединенными по Bluetooth.



22:01

Рис. 4.33. Типичный информационный кадр Bluetooth: а — на базовой скорости;

б — на увеличенной скорости

Бит F (Flow — поток) выставляется подчиненным узлом и сообщает о том, что его буфер заполнен. Этот бит обеспечивает примитивную форму управления потоком. Бит A (Acknowl—Acknowl—ed Element — подтверждение) представляет собой подтверждение (ACK), отсылаемое заодно с кадром. Бит S (Sequence — последовательность) используется для нумерации кадров, что позволяет обнаруживать повторные передачи. Это протокол с ожиданием, поэтому одного бита действительно оказывается достаточно.

23 March 2023

Артурия Пендрагон

16:43

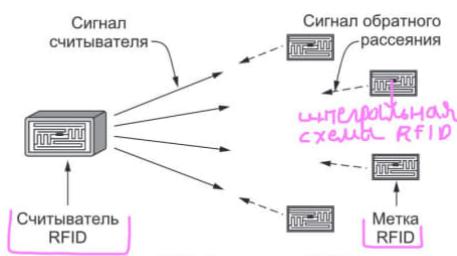


Рис. 4.34. Архитектура RFID

Class 1 – нет батареи, энергия от считывателя из радиопередачи

АП

Артурия Пендрагон

17:02

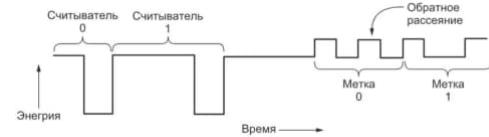
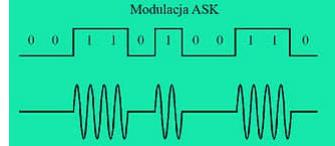


Рис. 4.35. Сигналы считывателя и сигналы обратного рассеяния от метки

№	Диапазон длии волн	Название диапазона волн	Диапазон частот	Название диапазона частот	Применение
1	100 Мм — 10 Мм	Декаметровые	3—30 Гц	Грайне низкие (ФН)	Сеть с под�权ами, профильческое исследование
2	10 Мм — 1 Мм	Миллиметровые	30—300 Гц	Срединные (СН)	Сеть с под�权ами, профильческое исследование
3	1000 мк — 100 мк	Гигаметровые	300—3000 Гц	Инфракрасные (ИР)	Сеть с под�权ами
4	100 мк — 10 мк	Миллиметровые	3—30 кГц	Сеть низких (ОН)	Следит тонкого времени, радиосвязь с под�权ами
5	10 мк — 1 мк	Биллиметровые	30—300 кГц	Низкие (Н)	Радиолокация, радиосвязь земной волны, радионавигация
6	1000 м — 100 м	Литометровые	300—3000 кГц	Средние (С)	Радиолокация и радиосвязь земной волны и ионосфера
7	100 м — 10 м	Декаметровые	3—30 МГц	Высокие (В)	Радиолокация и радиосвязь ионосферы, радиолокация, радио
8	10 м — 1 м	Метровые волны	30—300 МГц	Очень высокие (ОВ)	Телевидение, радиолокация, радиосвязь тропосферы и гравий волны, радио, ИК-терапия.

9	1000 мк — 100 мк	Декаметровые	300—3000 МГц	Ультракороткие (УКВ)	Телевидение, радиосвязь тропосферы и гравий волны, мобильные телефоны, радиолокация, медицинская микроволновая печь, спутниковая коммуникация
10	100 мк — 10 мк	Сантиметровые	3—30 Гц	Срединные (СН)	Радиолокация, интернет, спутниковая телекоммуникация, радиосвязь и радиолокация, прямой волны, беспроводные измерительные сети.
11	10 мк — 1 мк	Миллиметровые	30—300 Гц	Грайне высокие (ОН)	Радиолокация, высокоскоростная радиокомпьютерная сеть, радиолокация (метрополитенские, управление аэропортами), медицина, спутниковая радиосвязь.
12	Декаметровые	300—3000 Гц	Гигаметровые частоты, длинноволновая звуковая инфракрасного излучения	1.24 мк — 12.4 мк	Экспериментальная когерентная камера, когерентная изображение в оптике, когерентные измерения, излучение тепловоронными организмами, а также от более коротковолнового ИК излучения (излучение тепловороними материалами).

Артурия Пендрагон

17:21

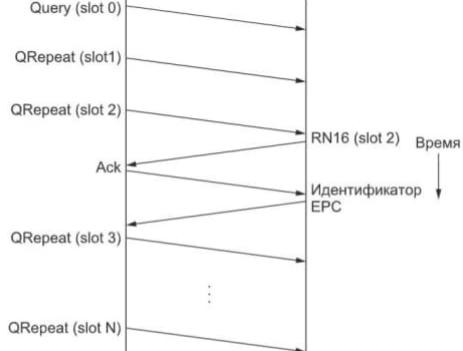


Рис. 4.36. Пример обмена сообщениями для идентификации метки

Артурия Пендрагон

21:15



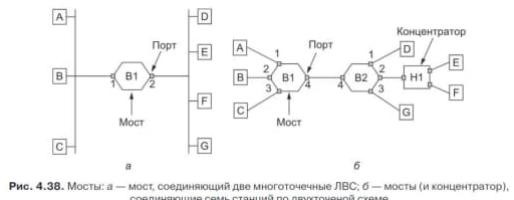
Рис. 4.37. Формат сообщения Query

25 March 2023

Артурия Пендрагон

16:55

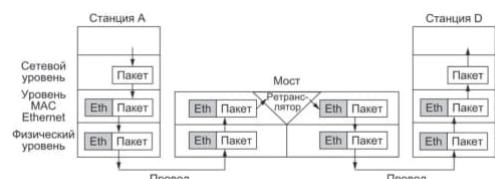
АП



Мосты— устройства, к которым присоединены станции и концентратор. Если технология ЛВС— Ethernet, мосты более известны под названием коммутаторы

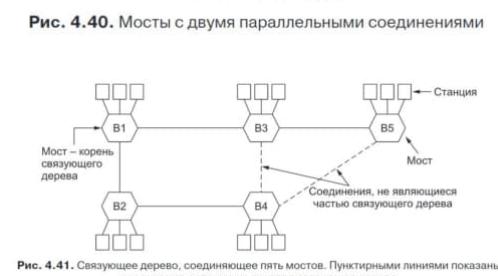
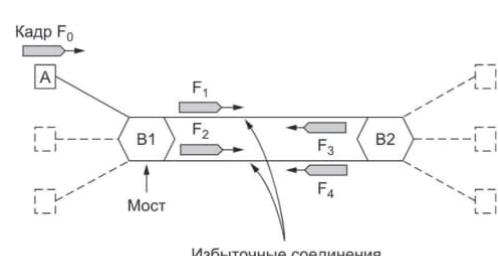
Артурия Пендрагон

17:58



Артурия Пендрагон

19:12



Артурия Пендрагон

19:48

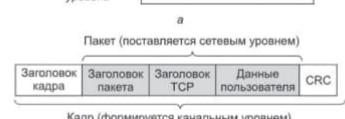
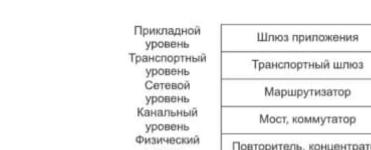
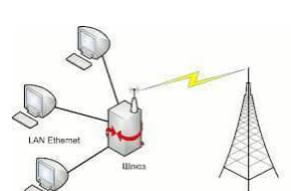


Рис. 4.42. Соответствие устройств уровням (а); кадры, пакеты и заголовки (б)



19:48

Шлюз (gateway) в компьютерных сетях – это устройство или программа, которая соединяет разные сети и позволяет им обмениваться данными. Шлюз может выполнять функции маршрутизации трафика между сетями, а также преобразования протоколов, например, переводя данные из одного формата в

другой. Обычно шлюзы используются для соединения локальной сети с интернетом, или для связи нескольких локальных сетей в одну общую сеть.

Артурия Пендрагон

20:18

АП

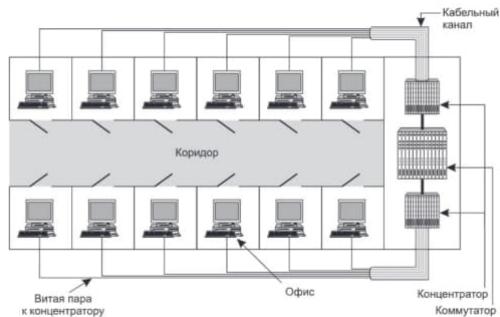


Рис. 4.43. Здание с централизованной проводкой с использованием концентратора и коммутатора

26 March 2023

Артурия Пендрагон

12:25

АП

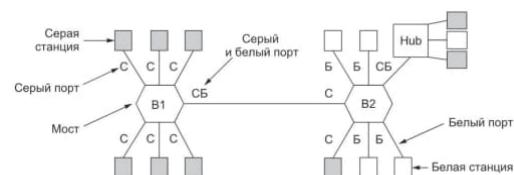


Рис. 4.44. Две виртуальные сети, серая и белая, в сети с мостом

Артурия Пендрагон

12:51

АП

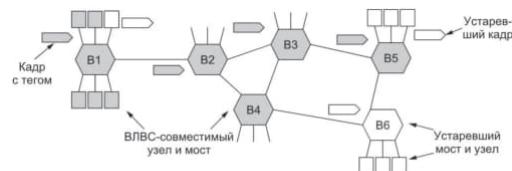


Рис. 4.45. ЛВС с мостами, частично совместимая с ВЛВС. Затененные символы — это ВЛВС-совместимые устройства. Все остальные не совместимы с виртуальными сетями



Рис. 4.46. Форматы кадров Ethernet-стандартов 802.3 и 802.1Q

12:53

27 March 2023

Артурия Пендрагон

16:14

<https://www.upwork.com/ab/portfolios/details>

Артурия Пендрагон

21:12

АП

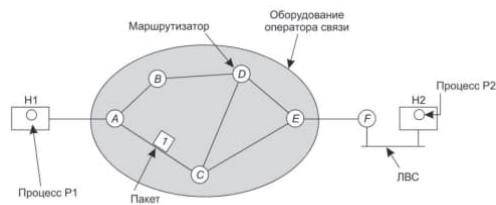


Рис. 5.1. Окружение, в котором функционируют протоколы сетевого уровня

28 March 2023

АП

Артурия Пендрагон

19:25

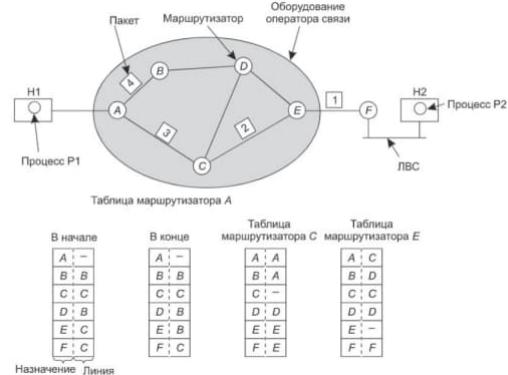


Рис. 5.2. Маршрутизация внутри дейтаграммной подсети

дейтаграммами – но конект, независимый маршрут пакетов.
виртуальным каналом (VC, Virtual Circuit) – конект до начала и до
конца

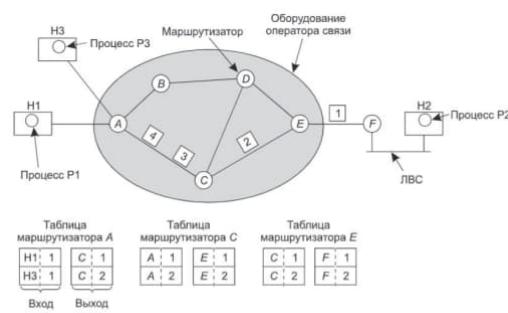


Рис. 5.3. Маршрутизация в сети виртуального канала

АП

Артурия Пендрагон

20:18

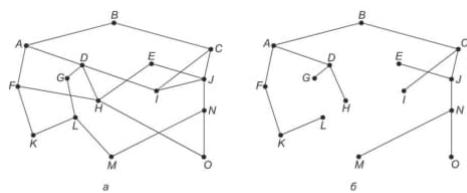
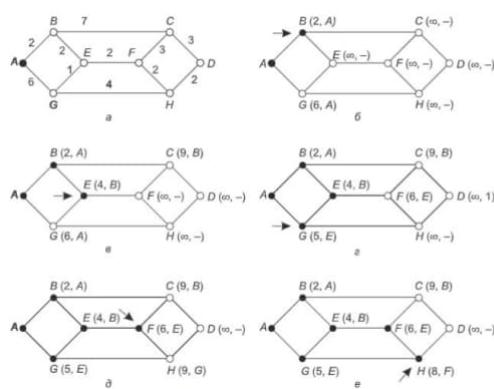


Рис. 5.5. Сеть (а); входное дерево для маршрутизатора B (б)

АП

Артурия Пендрагон

21:19

Рис. 5.6. Первые шесть шагов вычисления кратчайшего пути от А к D.
Стрелка указывает на рабочий узел

29 March 2023

АП

Артурия Пендрагон

12:36

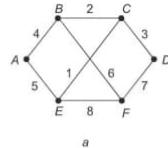
Беллмана—Форда == алгоритм маршрутизации по вектору расстояний

Конвергенция – установление маршрутов, соответствующих кратчайшим путям, в сети (convergence) 12:37

Артурия Пендрагон

20:00

АП



а

Пакеты состояния линий					
A	B	C	D	E	F
Порядковый номер	Порядковый номер	Порядковый номер	Порядковый номер	Порядковый номер	Порядковый номер
Возраст	Возраст	Возраст	Возраст	Возраст	Возраст
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
F 6	E 1			F 8	E 8

б

Рис. 5.10. Сеть (а); пакеты состояния линий для этой сети (б)

Пакет начинается с идентификатора отправителя, за которым следует порядковый номер и возраст (описываемый ниже), а также список соседей

Артурия Пендрагон

21:53

АП

Источник	Порядковый номер	Возраст	Флаги отсылки			Флаги подтверждения			Данные
			A	C	F	A	C	F	
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Рис. 5.11. Буфер пакетов маршрутизатора В с рисунка 5.10

30 March 2023

Артурия Пендрагон

14:16

АП Некоторые из наиболее распространенных алгоритмов маршрутизации:

Маршрутизация по вектору расстояния (distance-vector routing) – каждый маршрутизатор отправляет информацию о маршрутах своим соседям, которые в свою очередь делают то же самое. Каждый маршрутизатор имеет таблицу маршрутизации, в которой для каждой сети указывается стоимость маршрута. Примером алгоритма маршрутизации по вектору расстояния является протокол RIP.

Маршрутизация с учетом состояния линий (link-state routing) – каждый маршрутизатор отправляет информацию о состоянии своих линий своим соседям, которые передают эту информацию дальше. Каждый маршрутизатор использует эту информацию для расчета кратчайшего пути до каждой сети. Примером алгоритма маршрутизации с учетом состояния линий является протокол OSPF.

OSPF (Open Shortest Path First) – протокол маршрутизации, использующий алгоритм маршрутизации с учетом состояния линий. OSPF является протоколом с открытым исходным кодом, который широко используется в корпоративных сетях.

BGP (Border Gateway Protocol) – протокол маршрутизации, используемый для связи между автономными системами (AS). BGP

позволяет обмениваться информацией о маршрутах между разными провайдерами и AS, что позволяет строить более сложные сетевые архитектуры.

RIP (Routing Information Protocol) – протокол маршрутизации, использующий алгоритм маршрутизации по вектору расстояния. RIP является простым и легковесным протоколом, который широко использовался в небольших сетях.

EIGRP (Enhanced Interior Gateway Routing Protocol) – протокол маршрутизации, разработанный компанией Cisco. EIGRP объединяет преимущества алгоритмов маршрутизации по вектору расстояния и с учетом состояния линий, что позволяет быстро и эффективно строить маршруты.

IS-IS (Intermediate System to Intermediate System) – протокол маршрутизации, используемый для обмена информацией о маршрутах в сетях IP. IS-IS работает на уровне 2 и уровне 3 в модели OSI. Он используется для определения кратчайшего пути в сетях с большим количеством узлов и множеством возможных маршрутов.

PBR (Policy-based Routing) – технология маршрутизации, которая позволяет выбирать маршруты на основе определенных политик и условий, а не на основе обычных метрик маршрутизации, таких как пропускная способность или стоимость маршрута. PBR позволяет более гибко управлять трафиком и обеспечить более эффективное использование сетевых ресурсов.

HSRP (Hot Standby Router Protocol) – протокол, используемый для обеспечения высокой доступности в сетях IP. Он позволяет нескольким маршрутизаторам работать в режиме "горячей" резервирования, чтобы обеспечить автоматическое переключение на резервный маршрутизатор в случае отказа основного.

VRRP (Virtual Router Redundancy Protocol) – протокол, который также обеспечивает высокую доступность в сетях IP. Он позволяет нескольким маршрутизаторам работать в режиме виртуального маршрутизатора, который представляет собой единый IP-адрес и MAC-адрес. В случае отказа основного маршрутизатора, резервный маршрутизатор автоматически перехватывает трафик на себя. Отличие от HSRP заключается в том, что VRRP является стандартом IETF, в то время как HSRP разработан Cisco.

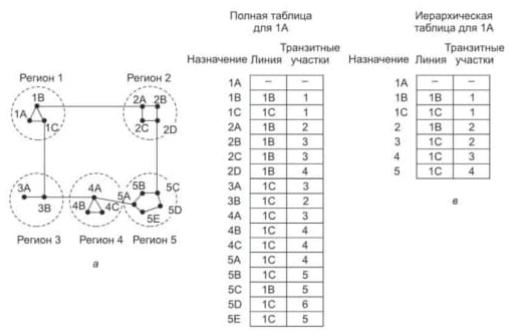
Артурия Пендрагон

14:51

АП
Патовая ситуация – это ситуация, когда две или более стороны находятся в тупике, не могут принять решение или договориться из-за противоречивых интересов или ограниченных возможностей. Это может привести к затяжной и неразрешимой конфликтной ситуации.

Иерархическая маршрутизация: *регионы* в кластеры, кластеры в зоны, зоны в группы

15:04



б

Рис. 5.12. Иерархическая маршрутизация

широковещанием (broadcasting) называется рассылка пакетов по всем пунктам назначения одновременно.

Артурия Пендрагон

15:41

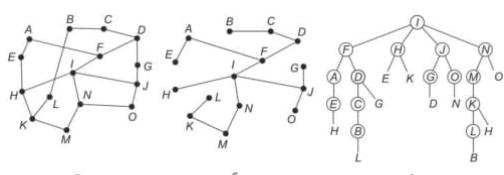


Рис. 5.13. Продвижение по встречному пути: а — сеть; б — входное дерево; в — дерево, построенное методом продвижения по встречному пути

Артурия Пендрагон

19:46

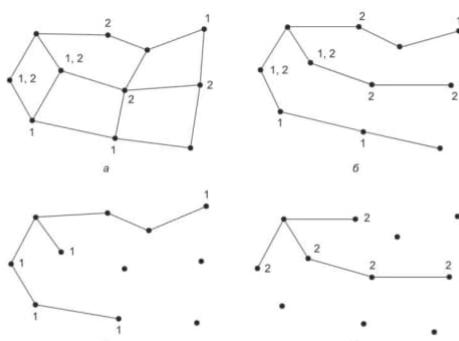


Рис. 5.14. Многоадресная рассылка: а — сеть; б — связующее дерево для самого левого маршрутизатора; в — многоадресное дерево для группы 1; г — многоадресное дерево для группы 2

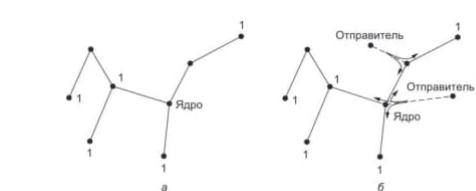


Рис. 5.15. Дерево с основанием в сердцевине для группы 1 (а); рассылка для группы 1 (б)

Артурия Пендрагон

20:00

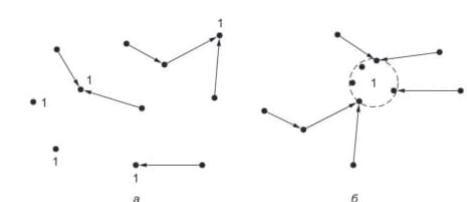
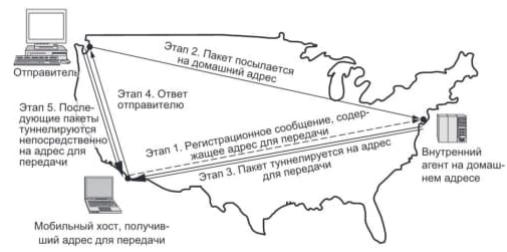


Рис. 5.16. Произвольная маршрутизация: а — маршруты для свободной рассылки; б — топология с точки зрения протокола маршрутизации

Артурия Пендрагон

20:42

АП



31 March 2023

Артурия Пендрагон

11:02

Выражение "звучит стоически" относится к философскому учению стоицизма, основными принципами которого являются принятие жизни такой, какая она есть, невмешательство во внешние обстоятельства и сохранение внутренней гармонии и спокойствия. Когда говорят, что что-то "звучит стоически", это может означать, что высказанное выражает подобные идеи о принятии того, что не может быть изменено, или о сохранении спокойствия и гармонии в любых обстоятельствах.

Артурия Пендрагон

16:31

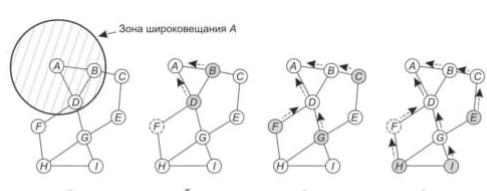


Рис. 5.18. Произвольная сеть: а — зона широковещания A; б — состояние после получения его узлами B и D; в — состояние после получения его узлами C, F и G; г — состояние после получения его узлами E, H и I. Затененными кружочками обозначены новые получатели. Пунктиром показаны возможные обратные маршруты. Сплошными линиями показан построенный маршрут

Артурия Пендрагон

17:19

Конвергенция – это процесс сближения или приближения различных элементов или систем

1 April 2023

Артурия Пендрагон

21:21

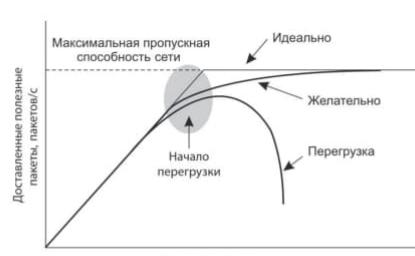


Рис. 5.19. При слишком высоком уровне трафика начинается перегрузка, и производительность сети резко снижается

2 April 2023

Артурия Пендрагон

11:52

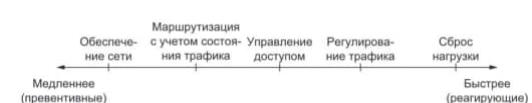


Рис. 5.20. Временные шкалы подходов к борьбе с перегрузкой

АП

Артурия Пендрагон

14:38

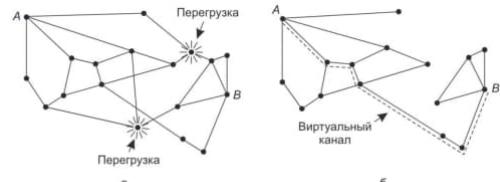


Рис. 5.22. Сеть: а — перегруженная; б — часть сети без перегрузки.
Показан виртуальный канал между А и В

АП

Артурия Пендрагон

17:56



Рис. 5.23. Явное уведомление о перегрузке

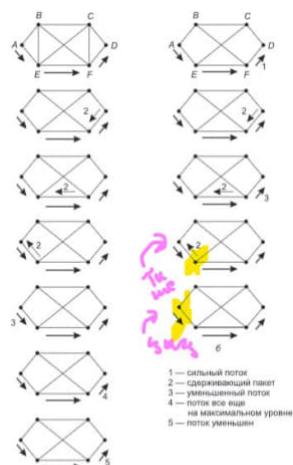


Рис. 5.24. Сдерживающий пакет влияет только на источник (а);
Сдерживающий пакет влияет на все промежуточные участки (б)

Первую стратегию (старое лучше нового) часто называют винной стратегией (маршрутизаторы), а вторую (новое лучше старого) — молочной стратегией (игры)

18:16

АП

Артурия Пендрагон

20:55

Последовательность пакетов, передающихся от источника к приемнику, называется потоком (Clark, 1988) (flow)

3 April 2023

АП

Артурия Пендрагон

08:18

<https://wiki.merionet.ru/seti/42/tipy-setevyx-atak/>

АП

Артурия Пендрагон

17:02

Колебание (то есть стандартное отклонение) времени задержки или времени прибытия пакета называется флюктуацией (jitter).

Постоянная битовая скорость — это попытка моделирования проводной сети путем предоставления фиксированной пропускной способности и фиксированной задержки.

Формирование трафика (traffic shaping) — способ регулировки средней скорости и равномерности потока входных данных.

На-блюдение за потоком трафика называется политикой трафика (traffic policing).

17:25



Рис. 5.25. Алгоритмы дырявого и маркерного ведра: а — формирование пакетов; б — дырявое ведро; в — маркерное ведро

$V + RS = MS$ — формула для расчета длительности максимальной выходной пачки данных

шайпер (формирователь) трафика

17:31

Артурия Пендрагон

18:09

Алгоритмы распределения ресурсов маршрутизатора между пакетами потока и кон-курирующими потоками называются алгоритмами диспетчеризации пакетов (packet scheduling algorithm)

Артурия Пендрагон

19:02

FIFO (First-In First-Out, первым пришел — первым ушел), или FCFS (First-Come First-Serve, первым пришел — первым обслуживается).

Артурия Пендрагон

19:49

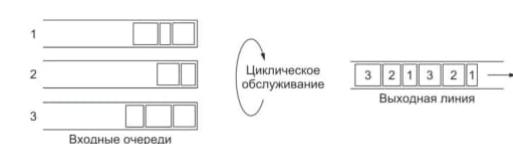


Рис. 5.27. Циклическое справедливое обслуживание

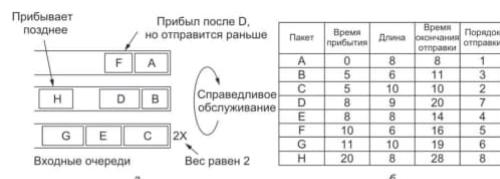


Рис. 5.28. Работа алгоритма: а — взвешенное справедливое обслуживание;

19:49

4 April 2023

Артурия Пендрагон

20:01

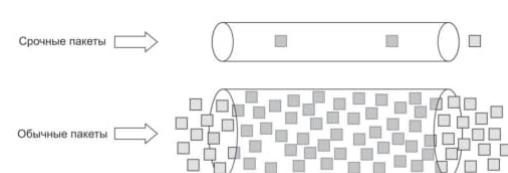


Рис. 5.32. Срочные пакеты движутся по свободной от трафика сети

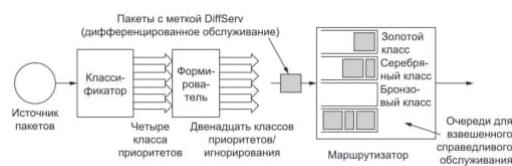


Рис. 5.33. Возможная реализация гарантированной пересыпалки потока данных

20:04

Артурия Пендрагон

22:41

АП



Рис. 5.34. Взаимодействие через сетевой слой: а — пакет проходит через разные сети;

б — выполнение протоколов на сетевом и канальном уровне

Коммутаторы не обязаны вникать в подробности устройства протокола сетевого уровня, с помощью которого производится коммутация. А маршрутизаторы — обязаны.

Маршрутизатор, поддерживающий несколько протоколов, называется мультипротокольным маршрутизатором (multiprotocol router)



Рис. 5.35. Туннелирование пакета из Парижа в Лондон

Транзитный участок – это участок дороги или маршрута, который не является начальным или конечным пунктом маршрута, а служит для проезда из одного места в другое. Транзитные участки часто связывают различные города, страны или континенты, и обычно на них находятся крупные транспортные узлы, такие как аэропорты, железнодорожные станции и порты.

In reply to this message 23:02



Рис. 5.36. Туннелирование автомобиля из Парижа в Лондон

оверлейная сеть – это сеть, создаваемая поверх уже существующей сети, которая позволяет обеспечивать связь и передачу данных между изолированными хостами.

В/За пределах/ми каждой сети для маршрутизации используется внутренний/внешний или внутридоменный/ междоменный. В сети Интернет междоменный протокол называется BGP(Border Gateway Protocol— пограничный межсетевой протокол)

Так как все сети управ-ляются независимо, они часто называются АС— автономными системами 23:11

5 April 2023

АП Артурия Пендрагон 21:30

MTU (Path Maximum Transmission Unit— максимальный размер пакета для выбранного пути)

разрешении шлюзам разбивать пакеты на фрагменты (fragments) и посыпать каждый фрагмент в виде отдельного пакета сетевого уровня.

21:44

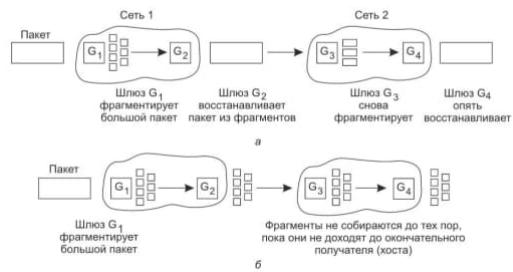


Рис. 5.37. Фрагментация: а — прозрачная; б — непрозрачная



Рис. 5.38. Фрагментация при элементарном размере 1 байт: а — исходный пакет, содержащий 10 байт данных; б — фрагменты после прохождения через сеть с максимальным размером 8 байт; в — фрагменты после прохождения через шлюз размером 5 байт



Рис. 5.39. Поиск путевого значения MTU

Артурия Пендрагон

22:25

Уильям Оккам (William Occam) декларировал этот принцип еще в XIV веке («Бритва Оккама»). Его можно выразить следующим образом:
Борись с излишествами.

Самые крупные магистрали (к которым необходимо присоединиться, чтобы получить доступ к остальной части сети Интер-нет) называются сетями Tier 1



Рис. 5.41. Заголовок IP-дейтаграммы IPv4

6 April 2023

Артурия Пендрагон

21:54

Префикс – это непрерывный блок пространства IP-адресов, который совпадает для всех хостов одной сети, такой как ЛВС Ethernet. Он определяет сетевую часть адреса и используется для маршрутизации пакетов в сети. 128.208.2.0 /24

Артурия Пендрагон

22:20



Рис. 5.42. Префикс IP-адреса и маска подсети

маска подсети выглядит так: 255.255.255.0

АП

Артурия Пендрагон

22:40

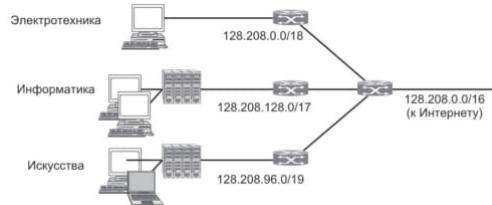


Рис. 5.43. Разделение IP-префикса при разбиении на подсети

Photo

22:40

1280×189

АП

Артурия Пендрагон

23:08

Агрегация маршрута (route aggregation) – это процесс объединения нескольких коротких IP-префиксов в один более длинный, более общий префикс, чтобы уменьшить размер таблиц маршрутизации и ускорить процесс маршрутизации в сети.

Длинный префикс, полученный в результате, иногда называют суперсетью (supernet),

Такой метод работает и для разбиения на подсети и называется CIDR (Classless InterDomain Routing — бесклассовая междоменная маршрутизация).

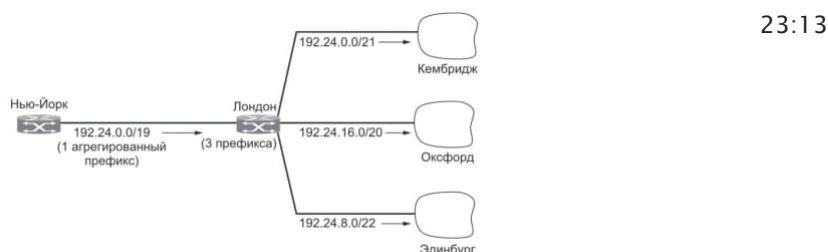


Рис. 5.44. Агрегация IP-префиксов

Таблица 5.6. Набор присвоенных IP-адресов

23:13

Университет	Первый адрес	Последний адрес	Количество	Форма записи
Кембридж	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Эдинбург	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Свободно)	194.24.12.0	194.24.15.255	1024	194.24.12.0/22
Оксфорд	194.24.16.0	194.24.16.255	4096	194.24.16.0/20

Согласно правилу, пакеты передаются в направлении самого специализированного блока, или самого длинного совпадающего префикса (longest matching prefix), в котором находится меньше всего IP-адресов.

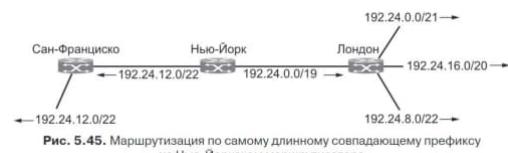


Рис. 5.45. Маршрутизация по самому длинному совпадающему префиксу на Нью-Йоркском маршрутизаторе

23:19

7 April 2023

АП

Артурия Пендрагон

19:04

Класс			Диапазон адресов хоста
A	0	Сеть	Хост
			От 1.0.0.0 до 127.255.255.255
B	10	Сеть	Хост
			От 128.0.0.0 до 191.255.255.255
C	110	Сеть	Хост
			От 192.0.0.0 до 223.255.255.255
D	1110	Адрес группы для многоадресной рассылки	
			От 224.0.0.0 до 239.255.255.255
E	1111	Зарезервировано для будущего использования	
			От 240.0.0.0 до 255.255.255.255

Рис. 5.46. Форматы IP-адреса

полноклассовой адресацией

19:05

Наконец, все адреса вида 127.xx.yy.zz зарезервированы для тестирования сетевого программного обеспечения методом обратной петли (loopback). Отправляемые по этому адресу пакеты не попадают на линию, а обрабатываются локально как входные пакеты. Это позволяет пакетам быть «посланными» на хост, когда отправитель на этом же хосте не знает его (своего) номера и даже если хост его не имеет, что может пригодиться для тестирования.

Артурия Пендрагон

19:33



Рис. 5.48. Расположение и работа NAT-блока

Артурия Пендрагон

23:36

версия Диринга (Deering) и Фрэнсиса (Francis), называемая в настоящий момент про-токолом SIPP (Simple Internet Protocol Plus — Простой интернет-протокол Плюс). Новому протоколу было дано обозначение IPv6.

8 April 2023

Артурия Пендрагон

17:07

Выражение "Совсем не изменилась. Совсем как кузнецик" обычно означает, что что-то осталось неизменным или не меняется со временем, как например, поведение или характер человека, несмотря на прошедшие годы.

Кузнецик, в свою очередь, известен своей способностью сохранять свою форму и структуру, несмотря на свою активность и жизненный цикл. Кроме того, кузнецик также ассоциируется с постоянством и регулярностью своих характеристик, таких как ритмичный звук, который они издают.

Таким образом, выражение "Совсем не изменилась. Совсем как кузнецик" обычно используется для описания качества или характеристик, которые остаются неизменными в течение длительного времени.

Артурия Пендрагон

18:09

АП Теория хаоса Жюля Пуанкаре – это область математики, изучающая динамические системы, в которых малые изменения начальных условий могут привести к значительным изменениям поведения системы в долгосрочной перспективе. Другими словами, теория хаоса изучает непредсказуемое поведение динамических систем.

Например, одной из простых динамических систем может быть маятник, который движется в пространстве под воздействием гравитации. Если маятник начнет движение с незначительно отличающихся начальных условий, то его движение со временем может стать значительно различным.

Теория хаоса изучает свойства и поведение таких систем. Она помогает понять, почему в природе могут возникать непредсказуемые и хаотические процессы, и как эти процессы могут быть описаны и поняты с помощью математических методов.

Артурия Пендрагон

18:45

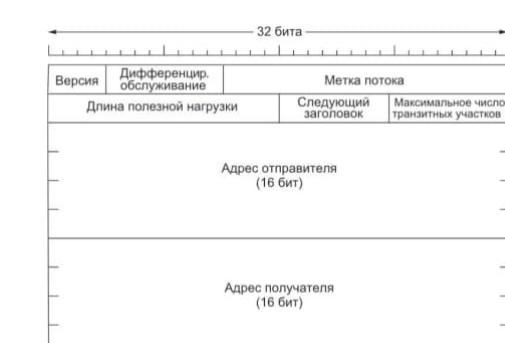


Рис. 5.49. Фиксированный заголовок IPv6 (обязательные поля)

Артурия Пендрагон

19:26

АП Адреса в IPv6 записываются в виде восьми групп по четыре шестнадцатеричных цифры, разделенных двоеточиями, например: 8000:0000:0000:0123:4567:89AB:CDEF

Поскольку многие адреса будут содержать большое количество нулей, были разрешены три метода сокращенной записи адресов. Во-первых, могут быть опущены ведущие нули в каждой группе, например 0123 можно записывать как 123. Во-вторых, одна или более групп, полностью состоящих из нулей, могут заменяться парой двоеточий. Таким образом, приведенный выше адрес принимает вид

:8000::123:4567:89AB:CDEF

Наконец, адреса IPv4 могут записываться как пара двоеточий, после которой пи-IPv4 могут записываться как пара двоеточий, после которой пи-4 могут записываться как пара двоеточий, после которой пи-шестся адрес в старом десятичном формате, например:
::192.31.20.46

Артурия Пендрагон

20:13

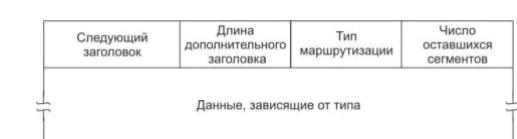


Рис. 5.51. Дополнительный заголовок для маршрутизации

АП

Артурия Пендрагон

20:36

Консенсус – это процесс достижения согласия между участниками, при котором каждый из них выражает свое мнение и в конечном итоге достигается единство в мнении или решении.

За работой Интернета следят маршрутизаторы. Если во время обработки пакета маршрутизатором случается что-то неожиданное, о происшествии сообщается по протоколу ICMP (Internet Control Message Protocol— протокол управляющих сообщений Интернета), используемому также для тестирования Интернета

Таблица 5.8. Основные типы ICMP-сообщений

Тип сообщения	Описание
Адресат недоступен	Пакет не может быть доставлен
Время истекло	Время жизни пакета упало до нуля
Проблема с параметром	Неверное поле заголовка
Гашение источника	Содержащий пакет
Переадресовать	Научить маршрутизатор географии
Запрос отклика и отклик	Проверить, живя ли машина
Запрос временного штампа и ответ	То же, что и отклик, но с временным штампом
Объявление маршрутизатора/запрос к маршрутизатору	Найти близлежащий маршрутизатор

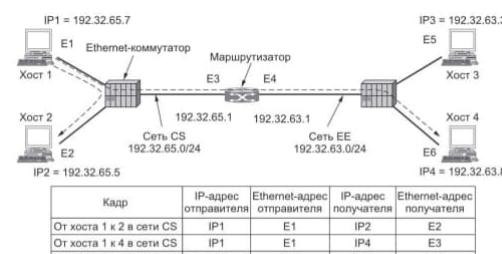
20:53

Ван Джейкобсоном в 1987 году, — утилита traceroute. Она находит маршрутизаторы, расположенные в узлах пути от хоста к адресу назначения. При этом ей не требуется особый уровень поддержки. Метод состоит в отправке на адрес назначения последовательности пакетов с временем жизни 1, 2, 3 и т. д. Маршрутизаторы, на которых счетчики достигают нуля, располагаются в том порядке, в котором пакет проходит их при пересылке. Эти маршрутизаторы послушно отправляют обратно на хост сообщения ВРЕМЯИСТЕКЛО. По этим сообщениям хост определяет их IP-адреса и получает информацию о пути.

Артурия Пендрагон

21:12

ARP — протокол разрешения адресов



21:13

Артурия Пендрагон

23:15

DHCP(Dynamic Host Configuration Protocol— протокол динамической настройки хостов)

9 April 2023

Артурия Пендрагон

10:51

Йоги Берра (Yogi Berra) – это легендарный американский бейсболист, тренер и персоналия в мире спорта. Он играл в национальной бейсбольной лиге (MLB) с 1946 по 1965 годы и был известен своим талантом, а также забавными и мудрыми высказываниями, которые стали называться "берризмами" ("Yogi-isms").

Один из наиболее известных "берризмов" – это "и снова это

дежавю". Это высказывание было сделано Беррой в 1964 году во время игры с командой Канзас-Сити Ройалс. Команда Нью-Йорк Янкиз, в которой играл Берра, играла против Ройалс и проигрывала 1–0. В конце 9-го inning, Берра забил ударом и выровнял счет, а затем его команда победила в экстратайме. После игры Берра рассказал журналистам: "это было как дежавю, все повторялось снова и снова". Высказывание стало известным и получило широкое распространение, став символом непредсказуемости и удивительности спорта.

"Берризмы" Йоги Берры, такие как "ничего не кончается, пока это не закончится", "это уже далеко не тот бейсбол, что был раньше" и другие, стали легендой в мире спорта и до сих пор часто цитируются в качестве примера остроумия и юмора.

MPLS (MultiProtocol Label Switching— мультипротокольная коммутация меток) и находится в опасной близости к коммутации каналов.—технология, позволяющая передавать интернет-трафик по сети.)



Рис. 5.53. Передача TCP-сегмента с использованием IP, MPLS и PPP

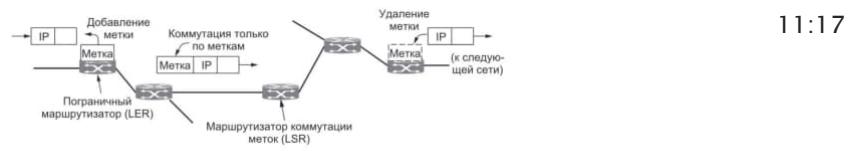


Рис. 5.54. Передача IP-пакета через MPLS-сеть

Артурия Пендрагон

АП

12:26

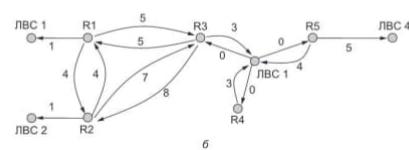
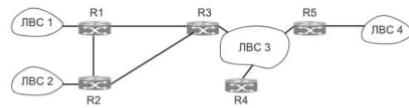


Рис. 5.55. Сеть множественного доступа: а — автономная система; б — представление (а) в виде графа

OSPF (Open Shortest Path First— открытый алгоритм предпочтительного выбора кратчайшего маршрута) протокол, учитывающий состояние линий, для внутриидоменной маршрутизации.

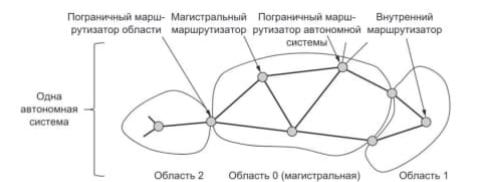


Рис. 5.56. Взаимосвязь между автономными системами, магистральными областями и областями в OSPF

Артурия Пендрагон

АП

13:03

Таблица 5.9. Пять типов сообщений протокола OSPF

Тип сообщения	Описание
Приветствие	Используется для знакомства с соседями
Обновление состояния каналов	Сообщает соседям информацию о каналах отправителя
Подтверждение состояния каналов	Подтверждает обновление состояния каналов
Описание базы данных	Сообщает о том, насколько свежей информацией располагает отправитель
Запрос состояния каналов	Запрашивает информацию у партнера

АП

14:33

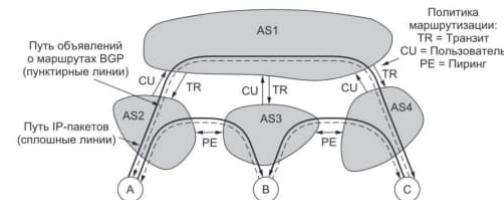
Артурия Пендрагон

Рис. 5.57. Политика маршрутизации между четырьмя автономными системами

Пиринг (англ. peer-to-peer, P2P) – это модель распределенной сети, в которой все узлы являются равноправными и обмениваются ресурсами напрямую, без посредничества центрального сервера. Это означает, что каждый узел может быть и клиентом, и сервером одновременно, обеспечивая функции как запроса, так и предоставления данных.

Транзит (англ. transit) – это прохождение через территорию, страну или регион без остановки или намерения остановиться там.

АП

15:08

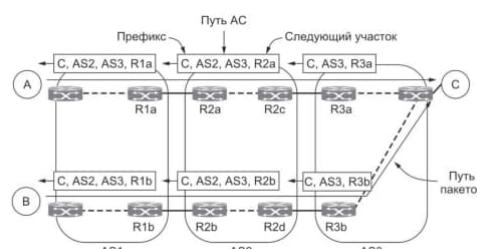
Артурия Пендрагон

Рис. 5.58. Распространение объявлений о BGP-маршруте

АП

17:00

Артурия Пендрагон

- ◆ 224.0.0.1 – все системы локальной сети;
- ◆ 224.0.0.2 – все маршрутизаторы локальной сети;
- ◆ 224.0.0.5 – все OSPF-маршрутизаторы локальной сети;
- ◆ 224.0.0.251 – все DNS-серверы локальной сети.

Диапазон IP-адресов [224.0.0.0/24](#) зарезервирован для многоадресной рассылки в локальной сети. Класс D

пограничные маршрутизаторы автономной системы (AS boundary router)

17:05

ECMP (Equal Cost MultiPath) – использование множества равноценных маршрутов

маршрутизатор коммутации меток (LSR, Label Switched Router)

Пограничный маршрутизатор(LER, Label Edge Router)

классу эквивалентности пересылок(FEC – Forwarding Equivalence Class)

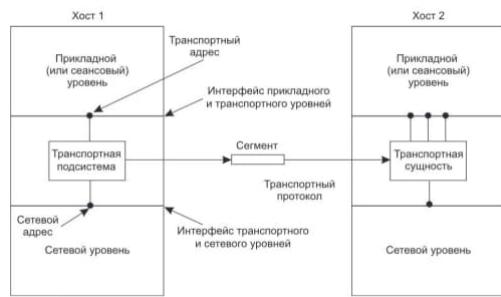
MPLS (MultiProtocol Label Switching— мультипротокольная коммутация меток)

IGMP (Internet Group Management Protocol— протокол управления группами в Интернете)

протокольно-независимая много-адресная рассылка (PIM, Protocol Independent Multicast)

Артурия Пендрагон

15:34



Артурия Пендрагон

18:19

сообщений, посылаемых одной транспортной подсистемой другой транспортной подсистеме, нам придется использовать термин **сегмент** (segment)

Таблица 6.1. Базовые операции простого транспортного сервиса

Базовая операция	Посланный сегмент	Значение
LISTEN (ОЖИДАТЬ) (нет)		Блокировать сервер, пока какой-либо процесс не попытается соединиться
CONNECT (СОЕДИНИТЬ)	CONNECTION REQUEST (ЗАПРОС СОЕДИНЕНИЯ)	Активно пытаться установить соединение
SEND (ПОСЛАТЬ)	ДАННЫЕ	Послать информацию
RECEIVE (ПОЛУЧИТЬ)	(нет)	Блокировать сервер, пока не прибудут данные
DISCONNECT (РАЗЪЕДИНИТЬ)	DISCONNECTION REQUEST (ЗАПРОС РАЗЪЕДИНЕНИЯ)	Прервать соединение

18:20



18:25

Сегменты, которыми обменивается транспортный уровень, помещаются в **пакеты** (которыми обменивается сетевой уровень). Эти пакеты, в свою очередь, содержатся в **кадрах**, которыми обменивается канальный уровень.

Артурия Пендрагон

18:43



Сокеты (sockets) в компьютерных сетях – это программный интерфейс (API), который позволяет приложениям взаимодействовать с сетевыми протоколами (например, TCP/IP) и передавать данные между компьютерами. С помощью сокетов приложения могут устанавливать сетевые соединения, отправлять и принимать данные в виде пакетов, управлять параметрами соединения и т.д.

18:47

18:50

Таблица 6.2. Базовые операции сокетов для TCP

Базовая операция	Значение
SOCKET (СОКЕТ)	Создать новый сокет (гнездо связи)
BIND (СВЯЗЫТЬ)	Связать локальный адрес с сокетом
LISTEN (ОЖИДАТЬ)	Объявить о желании принять соединение: указать размер очереди
ACCEPT (ПРИНЯТЬ)	Пассивно установить входящее соединение
CONNECT (СОЕДИНИТЬ)	Активно пытаться установить соединение
SEND (ПОСЛАТЬ)	Послать данные по соединению
RECEIVE (ПОЛУЧИТЬ)	Получить данные у соединения
CLOSE (ЗАКРЫТЬ)	Разорвать соединение

АП

Артурия Пендрагон

19:05

TCP(TransmissionControlProtocol — протокол управления передачей)
DCCP (Datagram Congestion Control Protocol— дейтаграммный протокол с управлением перегрузкой)
SCTP(Stream Control Transmission Protocol — протокол передачи с управлением потока-ми)
SST (Structured Stream Transport— иерархическая поточная транспортировка данных)

АП

Артурия Пендрагон

20:02

SERVER_PORT от 1024 до 65535 порты с номерами 1023 и ниже зарезервированы для привилегированных пользователей.

АП

Артурия Пендрагон

20:21

Если она называется client, ее типичный вызов будет выглядеть так:client flits.csvu.nl /usr/tom/filename >f

имя сервера (например, flits.cs.vu.nl) и переводится в IP-адрес 20:22 с помощью gethostbyname. Для поиска имени функция использует DNS.

```
Листинг 6.1. Программы использования сокетов для клиента и сервера
/* настройка созданного клиентского портами, запрашивает файл у серверной
программы, расположенной на следующей странице. */
/* Сервер в статике на запрос высылает файл. */

#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

#define SERVER_PORT 1234 /* По соглашению между клиентом и сервером */
#define BUF_SIZE 4096 /* Размер передаваемых блоков */

int main(int argc, char *argv)
{
    int c,i,bits;
    char buf[BUF_SIZE]; /*буфер для хранения файла*/
    struct hostent *h; /*информация о сервере*/
    struct sockaddr_in channel; /*канал*/
    channel.sin_family = AF_INET; /*указываем IP-адрес*/
    channel.sin_port = htons(SERVER_PORT); /*указываем порт*/
    channel.sin_addr.s_addr = htonl(INADDR_ANY); /*указываем IP-адрес*/

    if (argc<2) fatal("Для запуска введите: client имя_сервера имя_файла");
    h = gethostbyname(argv[1]); /*посыпаем IP-адреса хоста*/
    if (!h) fatal("Не удалось получить информацию о сервере");
    if (socket(PF_INET, SOCK_STREAM, IPPROTO_TCP))
        if (errno) fatal("Ошибка при создании сокета");
    if (bind(channel.sin_addr, &channel, sizeof(channel)))
        perror("bind");
    if (listen(channel, 5)) perror("listen");
    if (connect(&(struct sockaddr *) &channel, &channel, sizeof(channel)))
        if (errno) fatal("Ошибка соединения");
    if (send(channel.sin_port, "GET /index.html HTTP/1.1\r\n\r\n", 26) < 0)
        perror("send");
    /* Создано соединение. Попытка записи файла в кулерки байтам на конце */
    write(channel.sin_port, "GET /index.html HTTP/1.1\r\n\r\n", 26);
    /* Получить файл, записать на стандартное устройство вывода */
    while (1)
    {
        bytes = read(channel.sin_port, buf, BUF_SIZE); /* читать из сокета */
        if (bytes < 0) exit(0); /* проверка конца файла */
        write(1, buf, bytes); /* запись на стандартное устройство вывода */
    }
    fatal("main", string);
}
```

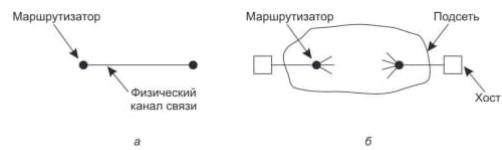
536–537 транспорт вр вр сокоры

20:33

```

main();
/* Наз программы для сервера */
#include <sys/types.h>
#include <sys/conf.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <sys/conf.h>
#include <sys/param.h>
#include <sys/errno.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <sys/conf.h>
#include <sys/param.h>
#include <sys/errno.h>
#define SERV_IP "192.168.1.100" /* IP-адрес сервера */
#define SERV_PORT 1234 /* Порт сервера */
#define BUFSIZE 4096 /* Размер передаваемых блоков */
#define QSIZE 10
int main(argc, argv, envp[])
{
    int s, b, fd, opt = 1;
    struct sockaddr_in server; /* Адрес для подключения клиента */
    struct sockaddr_in channel; /* Адрес для подключения сервера */
    /* Создать структуру адресов для приема в сокет */
    memset(&server, 0, sizeof(server)); /* Обнуление структуры */
    server.sin_family = AF_INET;
    server.sin_port = htons(SERV_PORT);
    server.sin_addr.s_addr = htonl(INADDR_ANY);
    channel.sin_port = htons(1234);
    /* Установка режима. Ожидание соединения */
    if (socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) == -1) /* Создать сокет */
    {
        perror("Error creating socket");
        exit(1);
    }
    if (bind(channel.sin_addr.s_addr, (struct sockaddr *)&channel, sizeof(channel)) == -1) /* Установка IP-адреса */
    {
        perror("Error binding socket");
        exit(1);
    }
    if (listen(QSIZE) == -1) /* Установка очереди */
    {
        perror("Error setting queue");
        exit(1);
    }
    /* Установка QSIZE... */ /* Определение размера очереди */
    if ((fd = accept(s, (struct sockaddr *)&server, &opt)) == -1) /* Установка соединения */
    {
        perror("Error accepting connection");
        exit(1);
    }
    /* Терминатор соединения и приказы. Ожидание и обработка соединения */
    while (1)
    {
        if (read(fd, &b, 1) == 1) /* Проверка в очереди запроса соединения*/
        {
            if (b == 'q') /* Установка доступа */
            {
                read(fd, buf, BUFSIZE); /* считать имя файла из сокета */
                /* Получить и вернуть файл */
                if (download(buf)) /* Открыть файл для отклика */
                {
                    if (b == 'd') /* Установка отклика файла */
                    {
                        write(fd, "OK", 3); /* Ответ на запрос */
                    }
                }
            }
            else if (b == 'r') /* Установка открытия файла */
            {
                read(fd, buf, BUFSIZE); /* Читать из файла */
                if (buf[0] == 'd') /* Установка нового файла */
                {
                    initbuf(buf); /* Запись файла в сокет */
                }
                else if (buf[0] == 'c') /* Закрыть файл */
                {
                    close(fd); /* Разорвать соединение */
                }
            }
        }
    }
}

```



20:36

Рис. 6.4. Окружение: а — канального уровня; б — транспортного уровня

Артурия Пендрагон

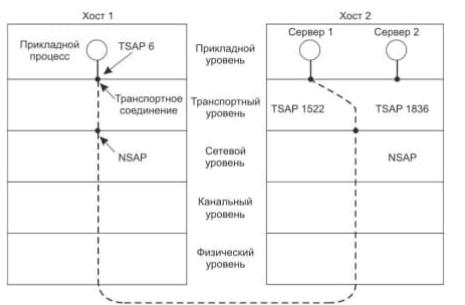
21:55

определении транспортных адресов, к которым процессы могут посылать запросы на установку соединения. В Интернете такие конечные точки называются портами. Мы будем пользоваться нейтральным термином TSAP (Transport Service Access Point — точка доступа к услугам транспортного уровня) для обозначения конечных точек на транспортном уровне. Аналогичные конечные точки сетевого уровня (то есть адреса сетевого уровня) называются NSAP (Network Service Access Point — точка доступа к сетевым услугам). Примерами NSAP являются IP-адреса.

In reply to [this message](#)

21:56

Порты — это транспортные адреса, которые используются для отправки запросов на установку соединения между процессами. Они являются конечными точками в Интернете, к которым процессы могут обращаться для обмена данными



22:04

Рис. 6.5. Точки доступа к услугам транспортного и сетевого уровня и транспортные соединения

в /etc/servicesUNIX-систем перечисляются серверы, за которыми UNIX-системы перечисляются серверы, за которыми — системы, перечисляются серверы, за которыми жестко закреплены определенные порты, с указанием этих портов — в частности, там указано, что почтовый сервер использует TCP порт 25.

22:16

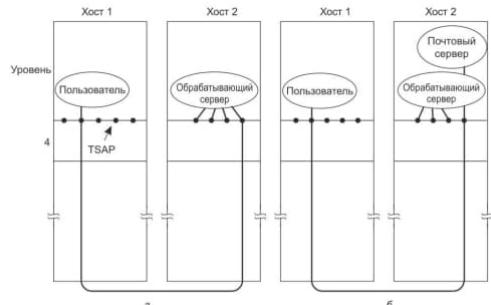


Рис. 6.6. Пользовательский процесс хоста 1 устанавливает соединение с почтовым сервером хоста 2 через обрабатывающий сервер

прокси (посредник)

22:21

11 April 2023

Артурия Пендрагон

12:56

Висновок. Вкажіть головні особливості машинобудування США, Канади та Бразилії.

Завдання 3 Вкажіть спільні і риси в структурі, обсягах виробництва та значенні окремих складових машинобудування США, Канади та Бразилії.

Спільні риси

Відмінні риси

Завдання 1 Вкажіть склад та значення машинобудування. 12:57

Завдання 2. Заповніть таблицю Порівняльна «Порівняльна характеристика машинобудування США, Канади та Бразилії» (за зразком). 12:58

Артурия Пендрагон

20:09

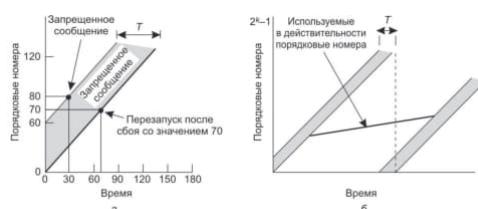


Рис. 6.7. Сегменты не могут заходить в запретную зону (а); проблема ресинхронизации (б)

Артурия Пендрагон

20:28

НАПОМИНАЛКА:

Принцип скользящего окна (Sliding Window) – это алгоритм управления потоком данных, используемый в протоколах передачи данных, таких как TCP (Transmission Control Protocol).

Он основан на идеи использования "окна" (window) для управления передачей данных между отправителем и получателем. Окно представляет собой определенное количество пакетов данных, которые могут быть отправлены отправителем без необходимости подтверждения получения каждого отдельного пакета.

При использовании протокола TCP, отправитель отправляет окно данных и ждет подтверждения получения этого окна от получателя, прежде чем продолжать отправку следующего окна. Получатель в свою очередь должен отправить подтверждение с номером последнего корректно полученного пакета данных. Если

АП

отправитель не получает подтверждение в течение определенного времени, он повторно отправляет неподтвержденные пакеты.

20:37

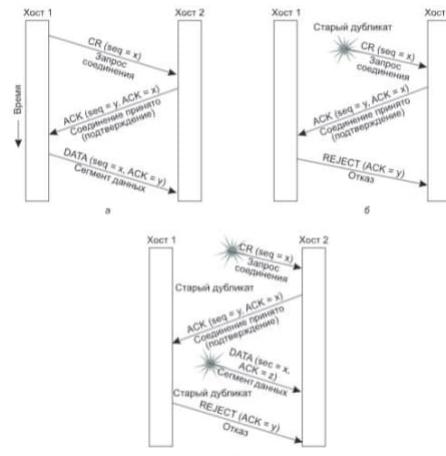


Рис. 6.8. Три сценария установки соединения с помощью «тройного рукопожатия» (CR означают CONNECTION REQUEST): а — нормальная работа; б — повторение старого дубликата CR; в — дубликат сегмента CR и дубликат сегмента ACK.

TCP использует «тройное рукопожатие» для установки соединения. Внутри соединения к 32-битному порядковому номеру добавляется метка времени, чтобы он не мог использоваться повторно в течение максимального времени жизни пакета, даже если скорость соединения составляет несколько гигабит в секунду. Этот механизм был добавлен в TCP для решения проблем, возникших при использовании быстрых линий. Он описан в RFC1323 и называется PAWS (Protection Against Wrapped Sequence numbers— детектирование повторного использования порядковых номеров)

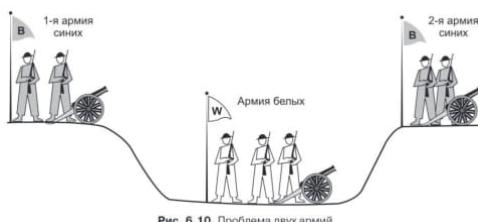
20:38



Рис. 6.9. Внезапное разъединение с потерей данных

существует два стиля разрыва соединения: асимметричный и симметричный. Асимметричный разрыв связи соответствует принципу работы телефонной системы: когда одна из сторон вешает трубку, связь прерывается. При симметричном разрыве соединение рассматривается в виде двух отдельных односторонних связей, и требуется раздельное завершение каждого соединения.

20:44



проблемой двух армий

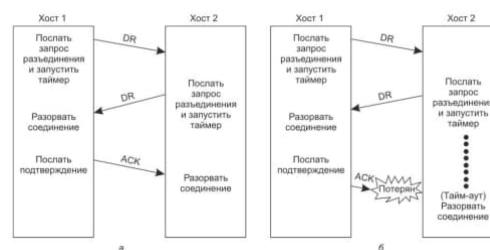
Представьте, что армия белых расположилась в долине, как

показано на рис. 6.10. На возвышенностях по обеим сторонам долины расположились две армии синих. Белая армия больше, чем любая из армий синих, но вместе синие превосходят белых. Если любая из армий синих атакует белых в оди-ночку, она потерпит поражение, но если синие сумеют атаковать белых одновременно, они могут победить. Синие армии хотели бы синхронизировать свое выступление. Однако единственный способ связи заключается в отправке вестового пешком по долине, где он может быть схвачен, а донесение потеряно (то есть приходится пользоваться ненадежным каналом). Спрашивается: существует ли протокол, позволяющий армиям синих по-бедить?

In reply to [this message](#)

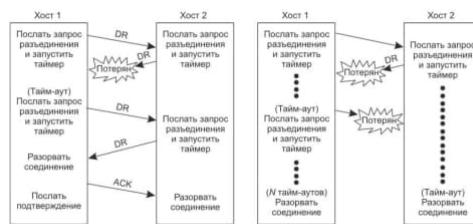
20:49

Чтобы увидеть, какое отношение проблема двух армий имеет к разрыву соединения, просто замените слово «атаковать» на «разъединить». Если ни одна сторона не готова разорвать соединение до тех пор, пока она не уверена, что другая сторона также готова к этому, то разъединение не произойдет никогда.



20:55

Чтобы удалять полуоткрытые соединения, можно применять правило, гласящее, что если по соединению в течение определенного времени не прибывает ни одного сегмента, соединение автоматически разрывается.



20:55

Рис. 6.11. Четыре сценария разрыва соединения: а — нормальный случай «тройного рукопожатия»; б — потерян последнее подтверждение; в — потерян ответ; г — потерян ответ и последующие запросы

хотя TCP обычно использует симметричный разрыв связи (при этом каждая сторона независимо прерывает свое соединение, отправляя пакет FIN после окончания передачи данных), веб-серверы часто передают клиентам специальный пакет RST, сообщающий о мгновенном разрыве соединения — что больше похоже на асимметричный разрыв.

CRC-код или контроль-CRC-код или контроль--код или контроль-ную сумму

21:03

Артурия Пендрагон

21:42

ARQ (Automatic Repeat reQuest — автоматический запрос повторной передачи)

«сквозной» принцип (end-to-end argument): Согласно этому принципу, сквозная проверка, выполняемая на транспортном уровне, является необходимой для корректной передачи данных; проверка, выполняемая на канальном уровне, не является необходимой, но позволяет существенно улучшить

производительность (так как иначе поврежденный пакет будет все равно проходить весь путь, что приведет к лишней нагрузке на сеть)

АП

Артурия Пендрагон

22:09

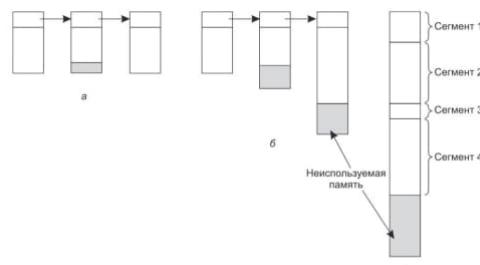


Рис. 6.12. Организация набора буферов: а — цепочка буферов фиксированного размера; б — цепочка буферов переменного размера; в — один большой циклический буфер для одного соединения

АП

Артурия Пендрагон

22:41

A	Сообщение	B	Комментарии
1	→ < request 8 buffers>	→	А хочет 8 буферов
2	← <ack = 15, buf = 4>	←	В позволяет переслать только сообщения 0–3
3	→ <seq = 0, data = m0>	→	У А теперь осталось 3 буфера
4	→ <seq = 1, data = m1>	→	У А теперь осталось 2 буфера
5	→ <seq = 2, data = m2>	***	Сообщение потерялось, но А думает, что у него остался 1 буфер
6	← <ack = 1, buf = 3>	←	В подтверждает получение сегментов 0 и 1, разрешает передачу со 2-го по 4-й
7	→ <seq = 3, data = m3>	→	У А остался 1 буфер
8	→ <seq = 4, data = m4>	→	У А осталось 0 буферов, и он должен остановиться
9	→ <seq = 2, data = m2>	→	У А истекло время ожидания, и он передает еще раз
10	← <ack = 4, buf = 0>	←	Все сегменты подтверждены, и он должен остановиться
11	← <ack = 4, buf = 1>	←	Теперь А может послать сегмент 5
12	← <ack = 4, buf = 2>	←	В где-то нашел новый буфер
13	→ <seq = 5, data = m5>	→	У А остался 1 буфер
14	→ <seq = 6, data = m6>	→	А снова блокирован
15	← <ack = 6, buf = 0>	←	А все еще блокирован
16	***	←	Потенциальный тупик

Рис. 6.13. Динамическое выделение буферов. Стрелками показано направление передачи. Многоточие (...) означает потерянный сегмент

12 April 2023

АП

Артурия Пендрагон

08:52

регенерація за рахунок клітин органа

АП

Артурия Пендрагон

09:19

регерація за рахунок клітин які оточують орган

як виражена здатність регенерації у рослин

09:19

АП

Артурия Пендрагон

15:56

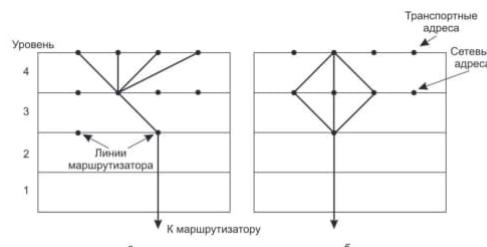


Рис. 6.14. Мультиплексирование: а — прямое; б — обратное мультиплексирование

Мультиплексирование – это процесс, при котором несколько потоков данных объединяются в один поток для передачи по одному каналу связи.

Примером обратного мультиплексирования является SCTP (Stream Control Transmission Protocol— протокол передачи с управлением потоками), позволяющий устанавливать соединение с множественными сетевыми интерфейсами.

АП

Артурия Пендрагон

16:17

		Стратегия, используемая получающим хостом		
		Сначала подтверждение, потом запись		
		Сначала записи, потом подтверждение		
Стратегия, используемая передающим хостом		AC(W)	AWC	C(AW)
Всегда повторять передачу		OK	DUP	OK
Никогда не повторять передачу		LOST	OK	LOST
Повторять передачу в S0		OK	DUP	LOST
Повторять передачу в S1		LOST	OK	OK
		OK	DUP	DUP
		LOST	OK	OK
		LOST	DUP	OK
		OK	OK	DUP

OK = Протокол работает корректно
DUP = Протокол формирует дубликат сообщения
LOST = Протокол теряет сообщение

Рис. 6.15. Различные комбинации стратегий сервера и клиента

отправка подтверждения (A), запись сегмента в выходной процесс (W) и сбой (C)

Артурия Пендрагон

17:06

мощность=нагрузка/задержка

Артурия Пендрагон

18:21

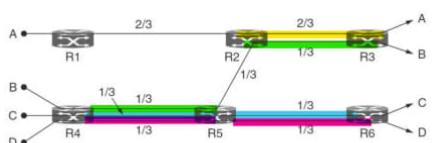


Рис. 6.17. Распределение пропускной способности по максиминному критерию для четырех потоков

Часто в сетях удобнее использовать форму равноправия, которая называется равнодоступностью по максиминному критерию. Это значит, что увеличение пропускной способности одного потока невозможно без уменьшения пропускной способности какого-либо другого потока с меньшей или равной пропускной способностью. Иными словами, от увеличения пропускной способности потока страдают менее «обеспеченные» потоки.

PS повышения 1 за счет снижения другого

Артурия Пендрагон

19:00

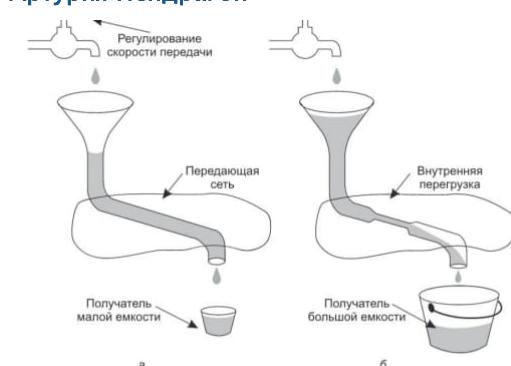


Рис. 6.19. Быстрая сеть и получатель малой емкости (а); медленная сеть и получатель большой емкости (б)

Таблица 6.3. Сигналы некоторых протоколов контроля насыщения

Протокол	Сигнал	Явный?	Точечный?
XCP	Скорость, которую следует использовать	Да	Да
TCP с ECN	Предупреждение о перегрузке	Да	Нет
FAST TCP	Сквозная задержка	Нет	Да
Compound TCP	Потеря пакетов и сквозная задержка	Нет	Да
CUBIC TCP	Потеря пакетов	Нет	Нет
TCP	Потеря пакетов	Нет	Нет

19:06

AIMD (Additive Increase Multiplicative Decrease — аддитивное увеличение мультипликативное уменьшение) — В отсутствие сигнала о насыщении отправители должны увеличивать скорость отправки, а при наличии такого сигнала — уменьшать.

In reply to this message

19:17

аддитивно — это относящееся к операции сложения

Например, если у пользователя была пропускная способность 1

Мбит/с, и он добавил 0,5 Мбит/с, то его новая пропускная способность станет равной 1,5 Мбит/с.

После достижения определенного уровня насыщения, пользователи начинают мультиплексивно уменьшать свою пропускную способность, что означает, что они уменьшают ее в процентном отношении к текущей пропускной способности. Например, если у пользователя была пропускная способность 1 Мбит/с, и он начал мультиплексивно ее уменьшать на 20%, то его новая пропускная способность станет равной 0,8 Мбит/с.

Артурия Пендрагон

19:32

Такая стратегия используется и в TCP. Если размер окна равен W , а круговая задержка — RTT , то эквивалентная скорость равна W/RTT .

Артурия Пендрагон

19:50

пропускная способность растет обратно пропорционально квадратному корню из скорости потери пакетов



Рис. 6.22. Контроль перегрузки для пути, содержащего беспроводной канал

сигнал/шум

20:07

Артурия Пендрагон

21:37

значение однобитных полей, называемых флагами, или кодовыми битами (code bits)

- URG — срочное сообщение;
- ACK — квитанция на принятый сегмент;
- PSH — запрос на отправку сообщения без ожидания заполнения буфера;
- RST — запрос на восстановление соединения;
- SYN — сообщение, используемое для синхронизации счетчиков переданных данных при установлении соединения;(само континъес)
- FIN — признак достижения передающей стороной последнего байта в потоке передаваемых данных.

Артурия Пендрагон

23:25

https://pikabu.ru/story/praktiki_po_kursu_kompyuternye_seti_bonus_4983902

13 April 2023

Артурия Пендрагон

10:52

2 Group up the words in the box according to the columns below.

tsunamis, droughts, blizzards, avalanches, tornadoes, hurricanes, floods, earthquakes, hailstorms, whirlpools, heat waves, landslides, fires, ice storms, volcanic eruptions, tornadoes

Land movement disasters

Water disasters

Weather disasters

Артурия Пендрагон

16:04

Протоколом без установления соединения является UDP (User Datagram Protocol — протокол передачидейтограммпользователя). Он не делает практически ничего, кроме отправки пакетов между приложениями, позволяя последним надстраивать свои собственные протоколы. TCP, напротив, является протоколом с установлением соединения. В его задачи входит практически все. Он устанавливает соединения и обеспечивает надежность сети, выполняя повторную передачу данных, а также осуществляет управление потоком данных и контроль перегрузки — и все это от лица приложений, которые его используют.



Рис. 6.23. Заголовок UDP

16:15

Поле Длина UDP состоит из заголовка и данных. Минимальная длина равна длине заголовка, то есть 8 байтам. Максимальная длина равна 65 515 байтам

Артурия Пендрагон

17:31



Рис. 6.24. Псевдозаголовок, включаемый в контрольную сумму UDP

TCP точно такоже

DNS (Domain Name System— служба имен доменов)

17:38

RPC (Remote Procedure Call— удаленный вызов процедур)

17:46

Традиционнозывающая процедура считается клиентом, а вызываемая — сервером. В простейшем случае для вызова удаленной процедуры клиентская программа должна быть связана с маленькой библиотечной процедурой, называемой клиентской заглушкой (client stub), которая отображает серверную процедуру в пространство адресов клиента. Аналогично сервер должен быть связан с процедурой, называемой серверной заглушкой (server stub). Эти процедуры скрывают тот факт, что вызов клиентом серверной процедуры осуществляется не локально. Упаковка параметров называется маршалингом (marshaling)

Артурия Пендрагон

18:09

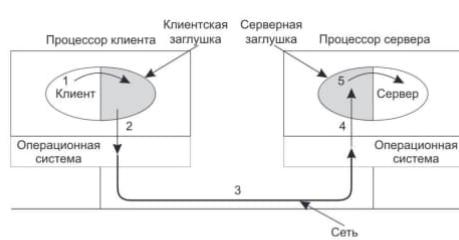


Рис. 6.25. Этапы выполнения удаленного вызова процедуры. Заглушки затенены

Шаг 1 заключается в вызове клиентом клиентской заглушки. Это локальный вызов процедуры, параметры которой самым обычным образом помещаются в стек. Шаг 2 состоит в упаковке параметров клиентской заглушки в сообщение и в осуществлении системного вызова для отправки этого сообщения. Упаковка параметров называется маршалингом (marshaling). На шаге 3 операционная система передает сообщение с клиентской машины на сервер. Шаг 4 заключается в том, что операционная система передает входящий пакет серверной заглушки. Последняя на пятом шаге вызывает серверную процедуру с распакованными параметрами. При ответе выполняются те же самые шаги, но передача происходит в обратном направлении.

Артурия Пендрагон

18:53

В контексте программирования идемпотентность означает, что выполнение операции несколько раз приводит к тому же результату, что и выполнение операции один раз.

RTP(Real-Time Transport Protocol — транспортный протокол реального масштаба времени) — это протокол передачи данных в реальном времени, который широко используется для передачи аудио и видео в интернете.

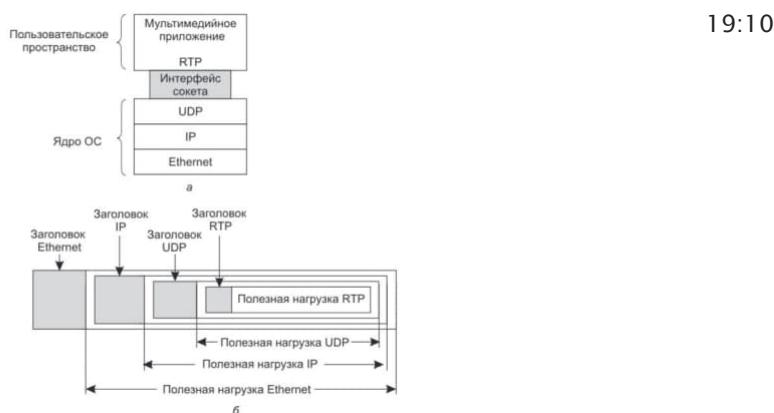


Рис. 6.26. RTP: а — положение RTP в стеке протоколов; б — вложение пакетов

Артурия Пендрагон

19:33

In reply to [this message](#)

PCM – это формат хранения звуковых сигналов в цифровом виде, в котором аналоговый звуковой сигнал отсчитается и преобразуется в последовательность цифровых значений. GSM – это сжатый формат аудио, который обычно используется для передачи голосовых сообщений в сотовых сетях. MP3 – это формат сжатия звука, который позволяет получить высокое качество звука при сравнительно низком объеме файла.

Артурия Пендрагон

19:52



Рис. 6.27. Заголовок RTP

Бит Р указывает на то, что размер пакета сделан кратным 4 байтам за счет байтов заполнения. При этом в последнем байте заполнения содержится общее число байтов заполнения. Бит X говорит о том,

что присутствует расширенный заголовок. Формат и назначение расширенного заголовка не определяются. Обязательным для него является только то, что первое слово расширения должно содержать общую длину расширения. Поле СС говорит о том, сколько сотрудничающих источников формируют поток. Их число может колебаться от 0 до 15. Бит М— это маркер, связанный с конкретным приложением. Он может использоваться для обозначения начала видео-кадра, начала слова в аудиоканале или еще для чего-нибудь, важного и понятного для приложения. Поле Тип данных содержит информацию об использующемся алгоритме кодирования (например, несжатое 8-битное аудио, MP3 и т. д.). Идентификатор источника синхронизации позволяет определить, какому потоку принадлежит пакет.

Джиттер (jitter) – это непредсказуемое изменение задержки в 19:59 передаче данных

[Артурия Пендрагон](#)

20:29

RTCP (Real-Time Transport Control Protocol — управляющий транспортный протокол реального времени) — Он занимается поддержкой обратной связи, синхронизацией, обеспечением пользовательского интерфейса, однако не занимается передачей каких-либо медиаданных.

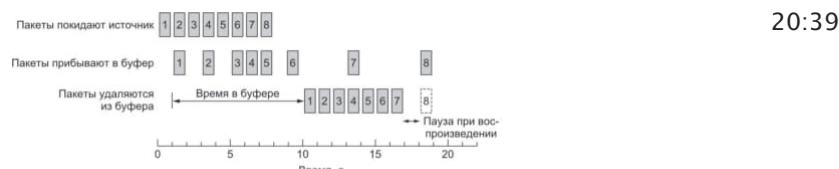


Рис. 6.28. Выравнивание выходного потока с помощью буферизации пакетов

сегментами речи (talkspurts), то есть во время пауз

20:43

задержка воспроизведения (playback point), то есть время, 20:44
которое получатель должен ждать медиаданных, прежде чем начать их воспроизведение

TCP (Transmission Control Protocol— протокол управления 20:58
передачей)

[Артурия Пендрагон](#)

22:31

Портом в TCP называют TSAP-адрес.

<https://www.iana.org/>

22:40

FTP-демон (FTP daemon) – это программа-сервер, которая 22:42
обеспечивает доступ к файлам на удаленном сервере через
протокол передачи файлов (FTP – File Transfer Protocol). FTP-демон
работает в фоновом режиме, ожидая запросы на соединение от
клиентских приложений, и отвечает на эти запросы, предоставляя
доступ к файлам на сервере.

Термин "демон" (daemon) в информатике обычно используется 22:44
для обозначения фоновой программы, которая работает в
операционной системе и выполняет определенные задачи без
непосредственного участия пользователя.

22:46

АП

Таблица 6.4. Некоторые зарезервированные порты

Порт	Протокол	Использование
20, 21	FTP	Передача файлов
22	SSH	Дистанционный вход в систему, замена Telnet
25	SMTP	Электронная почта
80	HTTP	Всемирная паутина (World Wide Web)
110	POP-3	Удаленный доступ к электронной почте
143	IMAP	Удаленный доступ к электронной почте
443	HTTPS	Защита от угроз (HTTP через SSL/TLS)
543	RTSP	Контроль воспроизведения мультимедиа
631	IPP	Коллективное использование принтера



Рис. 6.30. Четыре 512-байтовых сегмента, посланные как отдельные IP-дейтаграммы (а); 2048 байт данных, доставленные приложению с помощью одного вызова процедуры READ (б)

14 April 2023

АП

Артурия Пендрагон

14:19

максимальный размер передаваемого блока (MTU, Maximum Transfer Unit)

АП

Артурия Пендрагон

16:03

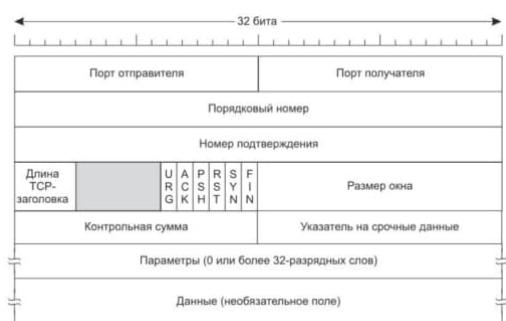


Рис. 6.31. Заголовок TCP

Каждый сегмент начинается с 20-байтного заголовка фиксированного формата. За ним могут следовать дополнительные поля (параметры). После дополнительных полей может располагаться до $65\ 535 - 20 - 20 = 65\ 495$ байт данных, где первые 20 байт — это IP-заголовок, а вто-IP-заголовок, а вто-заголовок, а вто-рые — TCP-заголовок. кортежем из пяти компонентов (5 tuple): протокол (TCP), IP-адрес источника, порт источника, IP-адрес полу-чателя и порт получателя.

CWR и ECE сообщают о перегрузках сети в случае, если используется явное уведомление о насыщении. Когда TCP-приемник узнает, что сеть перегружена, он с помощью флага ECE передает TCP-отправителю сигнал ECN-эхо, предлагая ему уменьшить скорость отправки. После того как TCP-приемник уменьшил скорость отправки, он сообщает об этом TCP-приемнику с помощью флага CWR с сигналом Окно насыщения уменьшено, после чего приемник перестает передавать сигнал ECN-эхо.

АП

Артурия Пендрагон

16:08

In reply to [this message](#)

АП

Артурия Пендрагон

16:52

факультативные поля имеют формат Тип–Длина–значение(в поле Параметры) + максимальный размер сегмента (MSS, Maximum Segment Size), который он может принять.

Детектирование повторного использования порядковых номеров (PAWS, Protection Against Wrapped Sequence numbers) удаляет сегменты со старыми метками времени(МЕТКИ ВРЕМЕНИ). выборочного подтверждения (SACK, Selective ACKnowledgement) получатель может сообщать отправителю диапазоны порядковых номеров доставленных пакетов

Артурия Пендрагон

19:20

АП

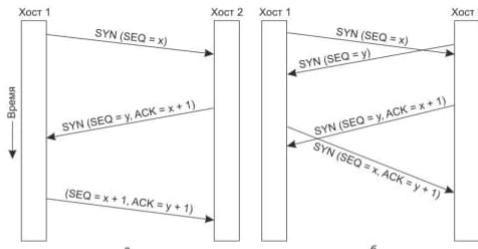


Рис. 6.32. Установка TCP-соединения в нормальном случае (а); одновременная установка соединения обеими сторонами (б)

пассивно ожидает LISTEN и ACCEPT

Другая сторона CONNECT, указывая IP-адрес и порт, с которым она хочет установить соединение, максимальный размер TCP-сегмента и, по желанию, некоторые данные пользователя

SYN cookies – это метод защиты от атак на TCP соединения, в частности, от атаки на установление соединения с использованием подделанных SYN-пакетов(затоплением SYN-сегментами (SYN flood)). SYN-атака основывается на том, что злоумышленник отправляет большое количество поддельных SYN-пакетов на сервер, не давая ему установить реальное соединение с другим устройством.

При использовании SYN cookies сервер создает криптографическое значение на основе данных из поддельного SYN-пакета, а затем записывает это значение в порядковый номер в исходящем SYN+ACK пакете. Этот порядковый номер не сохраняется на сервере и не занимает память на устройстве.

Если клиент ответил на SYN+ACK пакет с ACK пакетом, то сервер может вычислить порядковый номер, который он сгенерировал ранее, используя криптографический алгоритм, на основе данных из ACK пакета, и проверить правильность этого номера. Таким образом, сервер может проверить подлинность клиента и установить соединение, даже если он не сохранял порядковый номер.

Артурия Пендрагон

21:05

АП

Таблица 6.5. Состояния конечного автомата, управляющего TCP-соединением

Состояние	Описание
CLOSED	Закрыто. Соединение не является активным и не находится в процессе установления
LISTEN	Ожидание. Сервер ожидает входящего запроса
SYN RCVD	Прибыл запрос соединения. Ожидание подтверждения
SYN SENT	Запрос соединения послан. Приложение начало открывать соединение
ESTABLISHED	Установлено. Нормальное состояние передачи данных
FIN WAIT 1	Приложение сообщило, что ему больше нечего передавать
FIN WAIT 2	Другая сторона согласна разорвать соединение
TIME WAIT	Ожидание, пока в сети не исчезнут все пакеты
CLOSING	Обе стороны попытались одновременно закрыть соединение
CLOSE WAIT	Другая сторона инициировала разъединение
LAST ACK	Ожидание, пока в сети не исчезнут все пакеты

Артурия Пендрагон

21:20

АП

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

Рис. 14.1. Иерархическая структура стека TCP/IP



Рис. 14.2. Названия протокольных единиц данных в TCP/IP

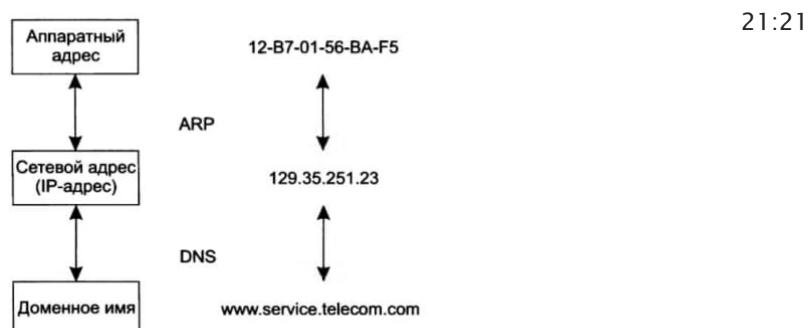


Рис. 14.3. Преобразование адресов

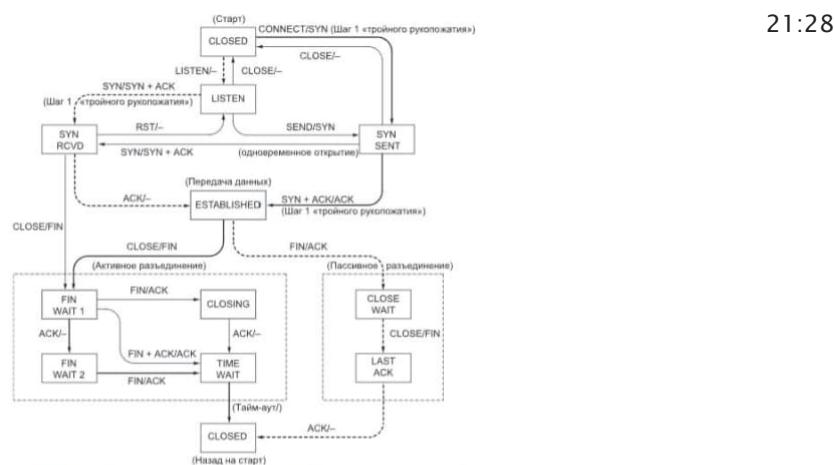


Рис. 6.33. Конечный автомат TCP-соединения. Жирная сплошная линия показывает нормальный путь клиента. Жирным пунктиром показан нормальный путь сервера. Тонкими линиями обозначены необычные события

Артурия Пендрагон

алгоритм Нагля (Nagle's algorithm) (Nagle, 1984). Предложение Нагля звучит довольно просто: если данные поступают отправителю маленькими порциями, отправитель просто передает первый фрагмент, а остальные помещает в буфер, пока не будет получено подтверждение приема первого фрагмента. После этого можно пере-слать все накопленные в буфере данные в виде одного TCP-сегмента и снова начать буферизацию до получения подтверждения о доставке следующего сегмента. Таким образом, в каждый момент времени может передаваться только один маленький пакет. Если за время прохождения пакета в оба конца приложение отправляет

АП

22:43

много порций данных, алгоритм Нагля объединяет несколько таких порций в один сегмент, и, таким образом, нагрузка на сеть существенно снижается. Кроме того, согласно этому алго-ритму новый пакет должен быть отправлен, если объем данных в буфере превышает максимальный размер сегмента.



Рис. 6.35. Синдром глупого окна

синдрома глупого окна (silly window syndrome) (Clark, 1982). Суть проблемы состоит в том, что данные пересылаются TCP-подсистемой крупными блоками, но принимающая сторона интерактивного приложения считывает их посимвольно. Чтобы ситуация стала понятнее, рассмотрим рис. 6.35. Начальное состояние таково: TCP-буфер приемной стороны полон (то есть размер его окна равен 0), и отправителю это известно. Затем интерактивное приложение читает один символ из TCP-потока. Принимающая TCP-подсистема радостно сообщает отправителю, что размер окна увеличился и что он теперь может послать 1 байт. Отправитель повинуется и посыпает 1 байт. Буфер снова оказывается полон, о чем получатель и извещает, посыпая подтверждение для 1-байтового сегмента с нулевым размером окна. И так может продолжаться вечно.

15 April 2023

Артурия Пендрагон

18:22

таймер повторной передачи (RTO, Retransmission TimeOut). Когда посыпается сегмент, запускается таймер повторной передачи. Если подтверждение получения сегмента прибывает раньше, чем истекает период таймера, таймер останавливается. Если же, наоборот, период ожидания ис-течет раньше, чем прибудет подтверждение, сегмент передается еще раз (а таймер запускается снова).

Дисперсия – это статистическая мера разброса данных относительно их среднего значения.

18:26

In reply to [this message](#)

18:30

Для каждого соединения в протоколе TCP предусмотрена переменная SRTT (Smoothed Round-Trip Time— усредненная круговая задержка), в которой хранится текущее наилучшее ожидаемое время получения подтверждения для данного соединения. При передаче сегмента запускается таймер, который замеряет время, требуемое для получения подтверждения, а также запускает повторную передачу, если подтверждение не приходит в срок. Если подтверждение успевает вернуться, прежде чем истечет период ожидания, TCP-подсистема замеряет время, потребовавшееся для его получения (R). Затем значение переменной SRTT обновляется по следующей формуле: $SRTT = \alpha SRTT + (1 - \alpha)R$, где α – весовой коэффициент, определяющий, насколько быстро забываются старые значения. Обычно он равен $7/8$. Эта формула — взвешенное скользящее среднее (EWMA, Exponentially Weighted Moving Average).

или фильтр низких частот, с помощью которого можно удалять шум.

Нетривиальный – это термин, используемый в различных областях, чтобы описать что-то, что не является очевидным 18:32

RTTVar (Round-Trip Time Variation, отклонение круговой задержки), которая вычисляется по формуле: 18:36

$$\text{RTTVar} = \beta \text{RTTVar} + (1 - \beta) |\text{SRTT} - R|.$$

Как и в предыдущем случае, это взвешенное скользящее среднее.

Как правило, $\beta = 3/4$. Значение интервала ожидания, RTO, устанавливается по формуле:

$$\text{RTO} = \text{SRTT} + 4 \times \text{RTTVar}.$$

<https://www.rfc-editor.org/rfc-index.html> 18:42

алгоритма Карна (Karn's algorithm) не обновлять оценки для переданных повторно пакетов. Кроме того, при каждой повторной передаче время ожидания можно удваивать до тех пор, пока сегменты не пройдут с первой попытки 18:45

таймером настойчивости (persistence timer). Он предназначен для предотвращения следующей тупиковой ситуации. Получатель посыпает подтверждение, в котором указывает окно нулевого размера, давая тем самым отправителю команду подождать. Через некоторое время получатель посыпает пакет с новым размером окна, но этот пакет теряется. Теперь обе стороны ожидают действий противоположной стороны. Когда срабатывает таймер настойчивости, отправитель посыпает получателю пакет с вопросом, не изменилось ли текущее состояние. В ответ получатель сообщает текущий размер окна. Если он все еще равен нулю, таймер настойчивости запускается снова, и весь цикл повторяется. Если же окно увеличилось, отправитель может передавать данные.

таймером проверки активности (keepalive timer). Когда соединение не используется в течение долгого времени, срабатывает таймер проверки активности, заставляя одну сторону проверить, есть ли еще кто живой на том конце соединения. Если проверяющая сторона не получает ответа, соединение разрывается. Эта особенность протокола довольно противоречива, поскольку она приносит дополнительные накладные расходы и может разорвать вполне жизнеспособное соединение из-за кратковременной потери связи. 18:48

таймер, запускаемый в состоянии TIME_WAIT конечного автомата при закрытии соединения. Он отсчитывает двойное время жизни пакета, чтобы гарантировать, что после закрытия соединения в сети не останутся созданные им пакеты. 18:49

Артурия Пендрагон 21:04

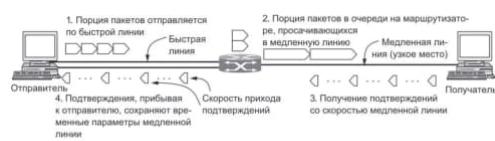


Рис. 6.37. Порция пакетов, переданная отправителем, и скорость прихода подтверждений

21:13

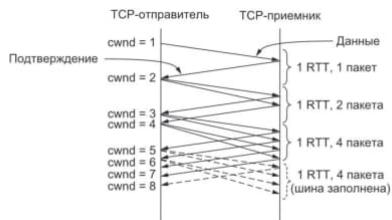


Рис. 6.38. Медленный старт с начальным окном перегрузки в один сегмент

медленный старт —|— порогом медленного старта

21:27

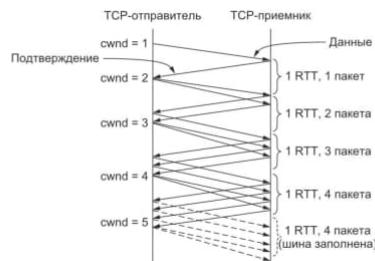


Рис. 6.39. Аддитивное увеличение при начальном окне размером один сегмент

16 April 2023

Артурия Пендрагон

11:53

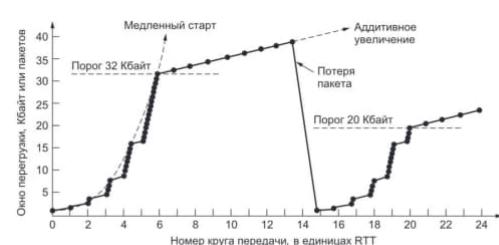


Рис. 6.40. Медленный старт и последующее аддитивное увеличение в TCP Tahoe

Артурия Пендрагон

12:28

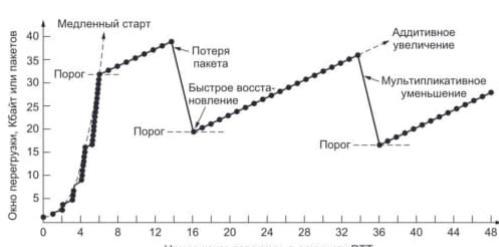


Рис. 6.41. Быстрое восстановление и пилообразный график для TCP Reno



При установлении соединения отправитель и получатель передают друг другу параметр SACK permitted, чтобы показать, что они могут работать с выборочными подтверждениями. Получатель использует поле Номер подтверждения обычным способом — как накопительное подтверждение последнего по порядку полученного байта. Когда пакет 3 приходит к нему вне очереди (так как пакет 2 потерян), он отправляет SACK option для полученных данных вместе с накопительным подтверждением (дубликатом) для пакета 1. SACK option содержит информацию о диапазонах полученных байтов, которые располагаются после номера самого подтверждения. Первый диапазон — пакет, к которому относится дубликат подтверждения. Следующие диапазоны, если они есть,

относятся к последующим блокам. Обычно используется не более трех диапазонов.

явных уведомлений о пере-грузке (ECN-эхо), Explicit Congestion Notification) ECE(с помощью флага ECE (ECN-эхо) сообщает отправителю о перегрузке) и CWR(Отправитель подтверждает получение этого сигнала с помощью флага CWR)

механизмы контроля перегрузки в TCP: 12:52
Оконный механизм контроля перегрузки (Window-based congestion control): TCP использует оконный механизм контроля перегрузки для динамической адаптации скорости передачи данных в сети. Этот механизм основан на изменении размера окна передачи данных в зависимости от количества потерянных пакетов и задержек в сети.

Slow-start: Это механизм контроля перегрузки, который позволяет установить начальное значение размера окна передачи данных. Он используется при установлении нового соединения или при обнаружении потери пакетов.

Congestion avoidance: Это механизм контроля перегрузки, который регулирует скорость передачи данных, когда окно передачи данных увеличивается и становится близким к максимальному значению. Он использует алгоритмы для предотвращения перегрузки в сети и снижения потерь пакетов.

Fast retransmit: Это механизм контроля перегрузки, который позволяет быстро переотправлять потерянные пакеты без необходимости ожидания таймера переотправки. Он используется при обнаружении потери пакетов, когда получатель отправляет дублированные ACK-пакеты.

Fast recovery: Это механизм контроля перегрузки, который позволяет быстро восстанавливаться после перегрузки сети, не уменьшая размер окна передачи данных. Он используется вместе с механизмом fast retransmit и позволяет сохранять производительность соединения, не снижая скорость передачи данных.

Explicit Congestion Notification (ECN): Это механизм, который позволяет маршрутизаторам в сети помечать пакеты, которые проходят через перегруженные участки сети. Когда получатель TCP получает помеченный пакет, он уменьшает скорость передачи данных, чтобы предотвратить перегрузку в сети.

Размер окна перегрузки (Congestion window): Это механизм, который определяет размер окна передачи данных в зависимости от состояния сети. Размер окна передачи данных может уменьшаться при обнаружении потери пакетов или увеличиваться при отсутствии потери пакетов.

АП Артурия Пендрагон 15:37

обращения к какому-нибудь DHCP-серверу (серверу динамической конфигурации хоста), чтобы узнать свой истинный адрес, а затем к файловому серверу, чтобы получить копию операционной системы

Артурия Пендрагон

21:10

АП

Порт отправителя	Порт получателя		
Порядковый номер		Версия IHL	
Номер подтверждения		Тип службы	Полная длина
Длина TCP-заголовка	Не используется	TTL	Контрольная сумма заголовка
Контрольная сумма	Указатель на срочные данные	Адрес отправителя	
Адрес получателя		Адрес получателя	

а

б

Рис. 6.46. TCP-заголовок (а); IP-заголовок (б). В обоих случаях затененные поля взяты у прототипа без изменений

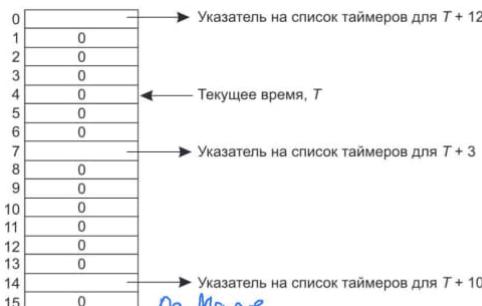


Рис. 6.47. Циклическое расписание

21:20

17 April 2023

Артурия Пендрагон

18:35

IP/UDP/RTP

Артурия Пендрагон

18:56

Про-пускная способность канала (в битах в секунду) умножается на время прохождения сигнала в оба конца (в секундах). В результате получается емкость канала в битах.

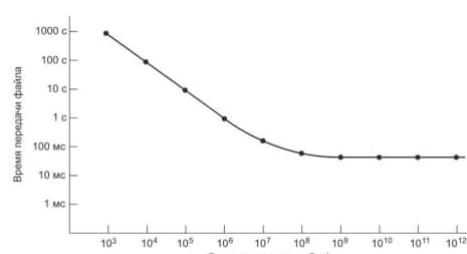


Рис. 6.49. Время передачи и подтверждения файла размером 1 Мбит по линии длиной 4000 км

19:06

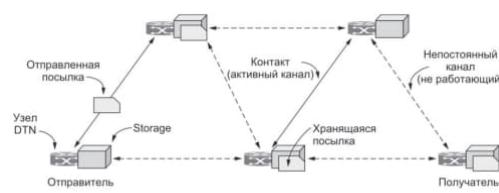
1 MIPS (1 млн инструкций в секунду)

19:14

Артурия Пендрагон

19:35

Тем не менее передача данных возможна и в сетях с непостоянной связью: эти данные могут задерживаться на узлах до тех пор, пока не появится рабочее соединение. Такой метод называется коммутацией сообщений. Сети, сконструированные по такому принципу, называются сетями, устойчивыми к задержкам (DTN, Delay-Tolerant Network), или распадоустойчивыми сетями (Disruption-Tolerant Network, DTN).



19:45

Рис. 6.50. Архитектура DTN

19:57



Рис. 6.51. Использование DTN в космосе

Артурия Пендрагон

21:11

АП



Рис. 6.52. Стек протоколов DTN



Рис. 6.53. Формат сообщений протокола Bundle

21:18

18 April 2023

Артурия Пендрагон

17:41

служба имен доменов (DNS, Domain Name System)

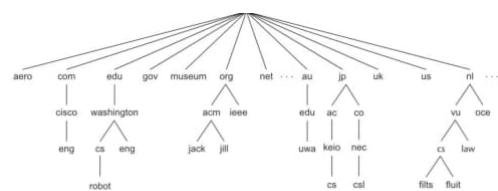


Рис. 7.1. Часть доменного пространства имен Интернета

17:55

Таблица 7.1. Родовые домены верхнего уровня

17:57

Домен	Использование	Дата основания	Ограниченный?
com	Коммерческие цели	1985	Нет
edu	Образовательные учреждения	1985	Да
gov	Правительство	1985	Да
int	Международные организации	1985	Да
mil	Военные	1985	Да
net	Сетевые провайдеры	1985	Нет
org	Некоммерческие организации	1985	Нет
aero	Авиатранспорт	2001	Да
biz	Бизнес	2001	Нет
coop	Кооперативы	2001	Да
info	Информация	2002	Нет
museum	Музеи	2002	Да
name	Люди	2002	Нет
pro	Профессионалы	2002	Да
cat	Каталоги	2005	Да
jobs	Занятость	2005	Да
mobi	Мобильные устройства	2005	Да
tel	Контактная информация	2005	Да
travel	Индустрия путешествий	2005	Да
xxx	Секс-индустрия	2010	Нет

Артурия Пендрагон

18:50

Японии домены [ac.jp](#) и [co.jp](#) соответствуют американским доменам [edu](#) и [com](#). В Голландии подобное различие не используется, и все домены организаций помещаются прямо под доменом [nl](#).

1. [cs.washington.edu](#) (Вашингтонский университет, США)

18:51

[cs.vu.nl](#) (университет Врийе, Нидерланды)

3. [cs.keio.ac.jp](#) (университет Кейо, Япония)

АП

Артурия Пендрагон

19:34

Таблица 7.2. Основные типы записей ресурсов DNS

Тип	Смысл	Значение
SOA	Начальная запись зоны	Параметры для этой зоны
A	IPv4-адрес хоста	Целое число, 32 двоичных разряда
AAAA	IPv6-адрес хоста	Целое число, 128 двоичных разрядов
MX	Обмен почтой	Приоритет, с которым домен желает принимать электронную почту
NS	Сервер имен	Имя сервера для этого домена
CNAME	Каноническое имя	Имя домена
PTR	Указатель	Псевдоним IP-адреса
SPF	Правила отправки почты	Правила отправки почты, закодированные в текстовом виде
SRV	Сервис	Хост, предоставляющий данный сервис
TXT	Текст	Не интерпретируемый ASCII-текст

Domain_name(обозначает домен, к которому относится текущая запись)

Time_to_live(указывает, насколько стабильно состояние записи. Редко 86400, непостоянный 60)

Class(Для информации Интернета значение этого поля всегда равно IN)

Type(означает тип DNS-записи)

Value

In reply to [this message](#)

19:38

Представим себе, что человек, знакомый в общих чертах с формированием имен в Интернете, хочет послать сообщение пользователю paul на отделении вычислительной техники Массачусетского технологического института (М.I.T.). Он может попытаться угадать нужный ему адрес, составив строку paul@cs.mit.edu. Однако этот адрес работать не будет, так как домен отделения вычислительной техники Массачусетского технологического института на самом деле называется csail.mit.edu. Таким образом, для удобства тех, кто этого не знает, М.I.T. может создать запись CNAME, позволяющую обращаться к нужному меню по обоим именам. Такая запись будет иметь следующий вид: cs.mit.edu 86400 IN CNAME csail.mit.edu

Листинг 7.1. Часть возможной базы данных домена cs.vu.nl

19:48

```
; Официальная информация для cs.vu.nl
cs.vu.nl. 86400 IN SOA star boss (9527,7200,7200,241920,86400)
cs.vu.nl. 86400 IN MX 1 zephyr
cs.vu.nl. 86400 IN MX 2 top
cs.vu.nl. 86400 IN NS star

star 86400 IN A 130.37.56.205
zephyr 86400 IN A 130.37.20.10
top 86400 IN A 130.37.20.11
www 86400 IN CNAME star.cs.vu.nl
ftp 86400 IN CNAME zephyr.cs.vu.nl

flits 86400 IN A 130.37.16.112
flits 86400 IN A 192.31.231.165
flits 86400 IN MX 1 flits
flits 86400 IN MX 2 zephyr
flits 86400 IN MX 3 top

rowboat 86400 IN A 130.37.56.201
rowboat 86400 IN MX 1 rowboat
rowboat 86400 IN MX 2 zephyr

little-sister 86400 IN A 130.37.62.23
laserjet 86400 IN A 192.31.231.216
```

Артурия Пендрагон

20:08

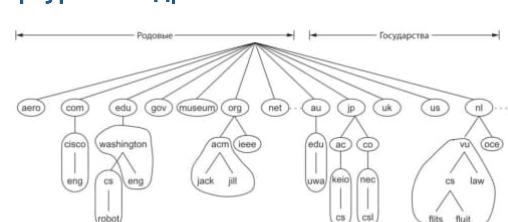


Рис. 7.2. Часть пространства имен DNS, разделенная на очерченные зоны

20:14

Exported Data

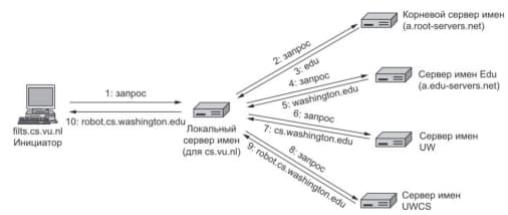


Рис. 7.3. Пример поиска распознавателем имени удаленного хоста в десяти шагах

авторитетную запись (authoritative record) ресурса. Авторитетной называют запись, получаемую от официального источника, хранящего данную запись и управляющего ее состоянием. Поэтому такая запись всегда считается верной, в отличие от кэшируемых записей (cached records), которые могут устаревать.

19 April 2023

Артурия Пендрагон

16:09

АП



Рис. 7.4. Архитектура системы e-mail

Артурия Пендрагон

17:13

АП

SMTP (Simple Mail Transfer Protocol — простого протокола передачи почтовых сообщений).

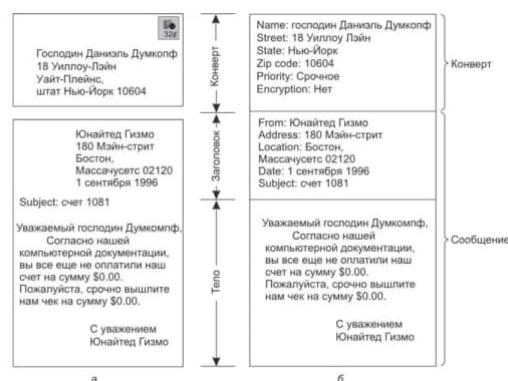


Рис. 7.5. Конверты и сообщения: а — обычное письмо; б — электронное письмо

Пользовательский агент — это программа (иногда называемая почтовым редактором — email editor или «читалкой» — email reader), управляемая множеством команд для составления и получения сообщений, а также для ответа на сообщения и управления почтовыми ящиками.

Артурия Пендрагон

17:30

АП

Адреса стандарта X.400 состоят из пар атрибут = значение, разделенных слэшами, например:

/C=US/ST=MASSACHUSETTS/L=CAMBRIDGE/PA=360 MEMORIAL
DR./CN=KEN SMITH/

Артурия Пендрагон

18:18

АП

Таблица 7.3. Поля заголовка стандарта RFC 5322, связанные с транспортировкой сообщения

Поле	Значение
To:	Электронный адрес (адреса) основного получателя (получателей)
Cc:	Электронный адрес (адреса) дополнительного получателя (получателей)
Bcc:	Электронный адрес (адреса) скрытой копии
From:	Автор (авторы) сообщения
Sender:	Электронный адрес отправителя
Received:	Строка, добавляемая каждым агентом передачи сообщений на протяжении маршрута
Return-Path:	Может быть использовано для идентификации обратного пути к отправителю

АП

Артурия Пендрагон

19:53

Таблица 7.4. Некоторые поля, используемые в заголовке сообщения стандарта RFC 5322

Поле	Значение
Date:	Дата и время отправки сообщения
Reply-to:	Электронный адрес, на который следует присыпать ответ
Message-Id:	Уникальный номер для последующей ссылки на это сообщение
In-Reply-To:	Идентификатор Message-Id сообщения, в ответ на которое посыпается это сообщение
References:	Другие важные ссылки (идентификаторы Message-Id)
Keywords:	Ключевые слова, выбираемые пользователем
Subject:	Краткое изложение темы сообщения для отображения в одной строке

АП

Артурия Пендрагон

20:16

MIME (Multipurpose Internet Mail Extensions — многоцелевые расширения электронной почты в Интернете)

20:19

Таблица 7.5. Заголовки сообщений, добавленные MIME

Заголовок	Описание
MIME-Version:	Указывает версию стандартов MIME
Content-Description:	Описание содержимого. Стока обычного текста, информирующая о содержимом сообщения
Content-Id:	Уникальный идентификатор
Content-Transfer-Encoding:	Указывает способ кодировки тела сообщения для его передачи
Content-Type:	Тип и формат содержимого сообщения

АП

Артурия Пендрагон

20:47

www.iana.org/assignments/media-types

MPEG (Motion Pictures Experts Group — экспертная группа по вопросам движущегося изображения)

20:56

Таблица 7.6. Типы стандарта MIME и примеры подтипов

Тип	Подтип	Описание
text	plain, html, xml, css	Текст в различных форматах
image	gif, jpeg, tiff	Изображения
audio	basic, mpeg, mp4	Звуки
video	mpeg, mp4, quicktime	Видеофильмы
model	vml	3D-модель
application	octet-stream, pdf, javascript, zip	Данные, производимые приложениями
message	http, rfc822	Инкапсулированное сообщение
multipart	mixed, alternative, parallel, digest	Комбинация нескольких типов

АП

Артурия Пендрагон

22:48

Знаменитый Розеттский камень был найден в 1799 году в Египте и содержал текст на трех языках – на древнеегипетском, греческом и демотическом. Этот камень стал ключом к расшифровке древнеегипетских иероглифов.

Листинг 7.2. Сообщение типа multipart, содержащее HTML и аудио

```
From: alice@cs.washington.edu
To: bob@ee.uwa.edu.au
MIME-Version: 1.0
Message-ID: <0704760941.AA00747@cs.washington.edu>
Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
Subject: Земля обвала вокруг Солнца целое число раз

Это преамбула. Пользовательский агент игнорирует ее. Ку-ку.

--qwertyuiopasdfghjklzxcvbnm
Content-Type: text/html

<p>Happy birthday to you<br>
Happy birthday to you<br>
Happy birthday to you</p>

--qwertyuiopasdfghjklzxcvbnm
Content-Type: message/external-body;
access-type="anon-ftp";
site="bicycle.cs.washington.edu";
directory="pub";
name="birthday.snd"

content-type: audio/basic
content-transfer-encoding: base64
--qwertyuiopasdfghjklzxcvbnm
```

20 April 2023

АП

Артурия Пендрагон

17:00

Использование SMTP с расширениями называется ESMTP (Extended SMTP — расширенный SMTP)

3 какахи в SMTP нет аунефикации, только ASCII(поэтому добавили MIMO – base64), не шифруется и никак не защищено.

Листинг 7.3. Передача сообщения от alice@cs.washington.edu для bob@ee.uwa.edu.au

```
S: 220 ee.uwa.edu.au служба SMTP готова
C: HELO abcd.com
S: 250 cs.washington.edu приветствует ee.uwa.edu.au
C: MAIL FROM: <alice@cs.washington.edu>
S: 250 подтверждено отправителя
C: RCPT TO: <bob@ee.uwa.edu.au>
S: 250 подтверждено получателя
C: DATA
S: 354 Отправляйте письмо: конец письма обозначается строкой, состоящей из символа "."
C: From: alice@cs.washington.edu
C: To: bob@ee.uwa.edu.au
```

C: MIME-Version: 1.0 17:07

```
C: Message-Id: <0704760941.AA00747@ee.uwa.edu.au>
C: Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
C: Subject: Земля обвала вокруг Солнца целое число раз
C:
C: Это прембула. Пользовательский агент игнорирует ее. Ку-ку.
C:
C: --qwertyuiopasdfghjklzxcvbnm
C: Content-Type: text/richtext
C:
C: Happy birthday to you
C: Happy birthday to you
C: Happy birthday dear <b>Carolyn</b> Carolyn </b>
C: Happy birthday to you
C:
C: --qwertyuiopasdfghjklzxcvbnm
C: Content-Type: message/external-body;
C: access-type="anon-ftp";
C: site="bicycle.cs.washington.edu";
C: directory="pub";
C: name="birthday.snd"
C:
C: content-type: audio/basic
C: content-transfer-encoding: base64
C: --qwertyuiopasdfghjklzxcvbnm
C:
S: 250 сообщение принято
C: QUIT
S: 221 ee.uwa.edu.au разрываю соединение
```

**Таблица 7.7.** Некоторые расширения SMTP

17:08

Ключевое слово	Описание
AUTH	Аутентификация клиента
BINARYMIME	Сервер принимает бинарные сообщения
CHUNKING	Сервер принимает большие сообщения по частям
SIZE	Проверка размера сообщения перед попыткой отсылки
STARTTLS	Переключение на безопасный канал (TLS; см. главу 8)
UTF8SMTP	Интернационализированный адрес

Клиенты, желающие использовать расширенную версию, в начале высыпают EHLO вместо HELO. Если этот вариант отвергается, сервер работает с обычным SMTP, а пользователь должен идти по стандартному пути. Если EHLO принимается, сервер отвечает, какие расширения он поддерживает. После этого клиент может использовать любое из перечисленных расширений.

Артурия Пендрагон

18:15

IMAP(Internet Mail Access Protocol — протокол доступа к электронной почте в Интернете)

IMAP — это улучшенная версия ранее разработанного протокола окончательной доставки POP3 (Post Office Protocol, version 3 — протокол почтового отделения, версия 3)

18:21

18:32

Таблица 7.8. Команды IMAP (версия 4)

Команда	Описание
CAPABILITY	Печатать возможности сервера
STARTTLS	Запустить безопасный транспорт (TLS, см. главу 8)
LOGIN	Войти на сервер, используя имя пользователя и пароль.
AUTHENTICATE	Авторизоваться иным способом
SELECT	Выбирать папку
EXAMINE	Выбирать папку, предназначенную только для чтения
CREATE	Создать папку
DELETE	Удалить папку
RENAME	Переименовать папку
SUBSCRIBE	Добавить папку к активному набору
UNSUBSCRIBE	Удалить папку из активного набора
LIST	Перечислить доступные папки
LSUB	Перечислить активные папки
STATUS	Узнать статус папки
APPEND	Добавить сообщение в папку
CHECK	Просмотреть состояние выбранной папки (что именно входит в понятие «состояние», зависит от конкретной реализации сервера). Создать контрольную точку для папки
FETCH	Просмотреть сообщения, находящиеся в папке
SEARCH	Найти сообщения, находящиеся в папке
STORE	Изменить метки сообщения
COPY	Сделать копию сообщения в папке
EXPUNGE	Удалить отмеченные сообщения
UID	Вызывать команды, используя уникальные идентификаторы
NOOP	Ничего не делать
CLOSE	Удалить помеченные сообщения и закрыть папку
LOGOUT	Выйти из системы и закрыть соединение

Всемирная паутина (WWW, WorldWideWeb, часто для краткости 18:44 просто «веб»)

Всемирная паутина была создана в 1989 году в Европейском 18:47 центре ядерных исследований CERN (Conseil European pour la Recherche Nucleaire) в Швейцарии.

Артурия Пендрагон

19:09

Эра доткомов – это период экономического роста и процветания в США, связанный с быстрым развитием интернет-технологий и созданием множества интернет-компаний в конце 1990-х – начале 2000-х годов. Многие из этих компаний были ориентированы на сферу электронной коммерции и получили огромный успех на фоне быстрого распространения интернета и растущей популярности онлайн-покупок. Однако, в результате пузыря интернет-рынка, многие из этих компаний обанкротились или сильно потеряли в цене, что привело к окончанию эры доткомов.

«пузыря доткомов»

В 1994 году CERN и Массачусетский технологический институт 19:12 (M.I.T., Massa-chussetts Institute of Technologies) подписали соглашение об основании WWW-консорциума (World Wide Web Consortium, иногда применяется сокращение W3C) — организации, цель которой заключалась в дальнейшем развитии Всемирной паутины, стандартизации протоколов и поощрении взаимодействия между отдельными сайтами.

<http://www.w3.org>

19:14

Артурия Пендрагон

19:43

URL (Uniform Resource Locator — унифицированный указатель информационного ресурса), который служит именем страницы во Всемирной паутине. URL делится на три части: протокол (который также называют схемой— scheme), DNS-имя машины, на которой расположена страница, и путь, уникально определяющий отдельную страницу (файл для чтения или программу, предназначенную для запуска на машине)

<http://www.cs.washington.edu/index.html>

19:46

Этот URL состоит из трех частей: протокола (http), DNS-имени хоста (www.cs.washington.edu) и имени пути (index.html).

In reply to [this message](#)

19:50

1. Браузер определяет URL (по выбранному элементу страницы).
2. Браузер запрашивает у службы DNS IP-адрес сервера www.cs.washington.edu
- .3. DNS дает ответ 128.208.3.88.
4. Браузер устанавливает TCP-соединение с 80-м портом (общезвестным портом для HTTP-протокола) машины 128.208.3.88.
5. Браузер отправляет HTTP-запрос на получение файла /index.html.
6. Сервер www.cs.washington.edu высылает страницу, как HTTP-ответ, например, от-правляя файл /index.html.
7. Если страница содержит URL, которые необходимы для отображения, браузер получает другие URL, используя тот же процесс. В этом случае URL включают множество размещенных изображений, также полученных с www.cs.washington.edu, размещенное видео с youtube.com и скрипт с google-analytics.com
- .8. Браузер отображает страницу /index.html в том виде, в котором она представлена на рис. 7.7.
9. Если в течение некоторого времени на те же серверы не поступает других запросов, TCP-соединения обрываются.

Таблица 7.9. Некоторые стандартные схемы URL

Имя	Используется	Пример
http	Гипертекст (HTML)	http://www.ee.uwa.edu/~rob/
https	Гипертекст с обеспечением безопасности	https://www.blank.com/~accounts/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Локальный файл	file:///usr/suzanne/prog.c
mailto	Отсыпка почты	mailto:JohnUser@icm.org
rtsp	Потоковая передача мультимедиа	rtsp://youtube.com/montypython.mpg
sip	Мультимедийный звонок	sip:eve@adversary.com
about	Информация браузера	about:plugins

19:55

Протокол ftp используется для доступа к файлам

было бы неплохо, если бы страницы, на которые идет множество ссылок, многократно копировались в разных частях сети, чтобы уменьшить трафик. Но мы не можем сказать: «Мне нужна страница хуз и мне все равно, откуда она возьмется». Чтобы решить эту проблему, URL были обобщены до URI (Uniform Resource Identifier — универсальный идентификатор ресурса). Некоторые URI указывают, как определить место нахождения ресурса. Это URL. Другие URI указывают имя ресурса, но не место его нахождения. Эти URI называются URN (Uniform Resource Name— унифицированное имя ресурса)

21 April 2023

Артурия Пендрагон

16:56

подключаемого модуля, плагина(plug-in)



16:59

Рис. 7.8. Браузер с подключаемым модулем (а); вспомогательное приложение (б)

Артурия Пендрагон

18:56

(После получения IP с DNS сервера):

1. Принимает входящее TCP-соединение от клиента (браузера).
2. Получает путь к странице, являющейся именем запрашиваемого файла.
3. Получает файл (с диска).
4. Высылает содержимое файла клиенту.
5. Разрывает TCP-соединение.

19:06

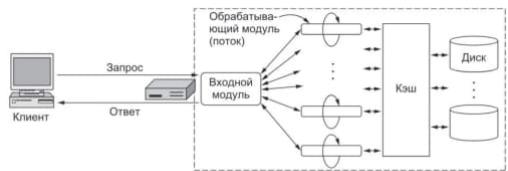


Рис. 7.9. Многопоточный веб-сервер с входным и обрабатывающими модулями

1. Вычисление имени запрашиваемой веб-страницы.2. 19:19
- Осуществление контроля доступа для веб-страницы.3. Проверка кэша.4. Получение запрошенной страницы с диска или запуск программы, создающей ее.5. Определение оставшейся части ответа (например, типа MIME).6. Возвращение ответа клиенту.7. Добавление записи в журнал активности сервера.

АП

Артурия Пендрагон

19:56

NAT (Network Address Translation) – это технология, которая позволяет скрыть сетевую адресацию устройств в локальной сети за одним или несколькими общедоступными IP-адресами.

DHCP – это протокол, который используется для автоматической настройки сетевых параметров устройств, подключенных к сети, в том числе IP-адреса, маски подсети, адреса шлюза по умолчанию и сервера DNS. DHCP позволяет избежать необходимости вручную настраивать каждое устройство в сети, что существенно упрощает работу сети и снижает вероятность ошибок в настройке.

АП

Артурия Пендрагон

21:36

Таблица 7.10. Несколько примеров cookie

Домен	Путь	Содержимое	Годен до	Защищенный
toms-casino.com	/	CustomerID=297793521	15-10-10 17:00	Да
jills-store.com	/	Cart=1-00501-1-07031-2-13721	11-1-11 14:22	Нет
aportal.com	/	Prefs=Stk;CSCO+ORCL;Spt;Jets	31-12-20 23:59	Нет
sneaky.com	/	UserID=4627239101	31-12-19 23:59	Нет

22 April 2023

АП

Артурия Пендрагон

19:23

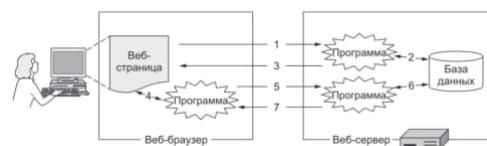


Рис. 7.12. Динамические страницы

АП

Артурия Пендрагон

19:40

API является методом обработки запросов динамических страниц. Он был до-ступен с момента возникновения Всемирной паутины. Он называется CGI(Common Gateway Interface— общий шлюзовой интерфейс).

PHP (PHP:Hypertext Preprocessor— PHP:Гипертекстовый препроцессор) Этот способ заключается во внедрении небольших скриптов в HTML-страницы. Они выполняются на сервере, в их задачу входит генерирование страницы

JSP (JavaServer Pages — Страницы сервера Java)

In reply to [this message](#)

19:44

1 action вызывает страницу которую построит сервер

2 action вызывает файл php

АП

Артурия Пендрагон

20:31

Листинг 7.9. Применение JavaScript для обработки формы

```
<html>
<head>
<script language="javascript" type="text/javascript">
function response(test_form) {
    var person = test_form.name.value;
    var years = eval(test_form.age.value) + 1;
    document.open()
    document.writeln("<html> <body>");
    document.writeln("Привет, " + person + " !<br>");
    document.writeln("В следующем году тебе будет " + years + ".");
    document.writeln("</body> </html>");
    document.close();
}
</script>
</head>

<body>
<form>
    Введите свое имя: <input type="text" name="name">
    <br>
    Введите свой возраст: <input type="text" name="age">
    <br>
    <input type="button" value="Подтверждение" onclick="response(this.form)">
</form>
</body>
</html>
```

717 из 960

апплетов (applets). Это небольшие программы на Java, скомпилированные в машинные инструкции виртуального компьютера, называемого JVM (Java Virtual Machine — виртуальная машина Java). Апплеты могут внедряться в HTML-страницы (между тегами `<applet>` и `</applet>`) и интерпретироваться JVM-совместимыми браузерами. Поскольку перед выполнением Java-апплеты проходят стадию интерпретации, интерпретатор может помочь избежать выполнения «нехороших действий». По крайней мере, теоретически такая возможность существует. На практике создатели апплетов обнаружили почти бесконечный поток ошибок в библиотеках ввода/вывода Java.

AJAX (Asynchronous JavaScript and XML — асинхронный JavaScript и XML) — Это набор технологий, которые работают совместно, чтобы создать веб-приложения, которые были бы такими же удобными и функциональными, как традиционные настольные прикладные системы.

Артурия Пендрагон

22:39

XSLT (eXtensible Stylesheet Language Transformations — стилевые трансформации расширяемого языка разметки) может использоваться для того, чтобы определить, каким образом трансформировать XML в HTML. XSLT похож на CSS, но у него гораздо больше возможностей.

<https://msiter.ru/tutorials/xslt>

22:42

Артурия Пендрагон

23:12

SOAP (Simple Object Access Protocol — простой протокол доступа к объектам), который является способом реализации веб-сервисов, выполняющих вызов удаленных процедур между программами, независимо от их языка и платформы.



23:17

Рис. 7.15. Различные технологии, используемые для создания динамических страниц.

23 April 2023

Артурия Пендрагон

АП

HTTP (HyperText Transfer Protocol— протокол передачи гипертекста)

12:41

АП

Артурия Пендрагон

13:01

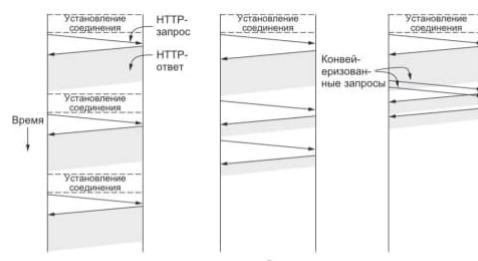


Рис. 7.16. HTTP: а — множественные соединения и последовательные запросы; б — постоянное соединение и последовательные запросы; в — постоянное соединение и конвейеризованные запросы

АП

Артурия Пендрагон

13:18

Таблица 7.12. Встроенные методы HTTP-запросов

Метод	Описание
GET	Запрос чтения веб-страницы
HEAD	Запрос чтения заголовка веб-страницы
PUT	Запрос сохранения веб-страницы
POST	Добавить к именованному ресурсу (например, к веб-странице)
DELETE	Удалить веб-страницу
TRACE	Отобразить входящий запрос
CONNECT	Зарезервирован для будущего использования
OPTIONS	Опрос определенных параметров

АП

Артурия Пендрагон

13:58

Таблица 7.13. Группы кодов состояния, содержащиеся в ответах сервера

Код	Значение	Примеры
1xx	Информация	100 = сервер согласен обрабатывать запросы клиента
2xx	Успех	200 = запрос успешно обработан; 204 = содержимое отсутствует
3xx	Перенаправление	301 = страница перемещена; 304 = кэшированная страница все еще доступна
4xx	Ошибка клиента	403 = ошибка доступа; 404 = страница не найдена
5xx	Ошибка сервера	500 = внутренняя ошибка сервера; 503 = попробуйте еще раз позднее

Таблица 7.14. Некоторые заголовки сообщений протокола HTTP

Заголовок	Тип	Содержимое
User-Agent	Запрос	Информации о браузере и его платформе
Accept	Запрос	Тип страницы, поддерживаемый клиентом
Accept-Charset	Запрос	Поддерживаемый клиентом набор символов
Accept-Encoding	Запрос	Поддерживаемый клиентом типы кодирования
Accept-Language	Запрос	Естественный язык, понимаемый клиентом
If-Modified-Since	Запрос	Время и дата последнего обновления
If-None-Match	Запрос	Текст, отправленный с последнего обновления
Host	Запрос	DNS-имя сервера
Authorization	Запрос	Список персональных идентификаторов клиента
Referer	Запрос	URL, с которого был отправлен предыдущий запрос
Cookie	Запрос	Отправка ранее принятого cookie-файла на сервер
Set-Cookie	Ответ	Сервер хочет, чтобы клиент сохранил cookie
Server	Ответ	Информация о сервере
Content-Encoding	Ответ	Тип кодирования содержимого (например, gzip)
Content-Language	Ответ	Естественный язык, используемый на странице
Content-Length	Ответ	Размер страницы в байтах
Content-Type	Ответ	Тип MIME страницы
Content-Range	Ответ	Идентифицирует часть контента страницы
Last-Modified	Ответ	Время и дата внесения последних изменений в страницу
Expires	Ответ	Время и дата, когда страница перестанет считаться действительной
Location	Ответ	Команда клиента на перенаправление его запроса по другому адресу
Accept-Ranges	Ответ	Сервер готов принимать запросы на страницы указанного размера
Date	Запрос/Ответ	Дата и время отправки сообщения
Range	Запрос/Ответ	Идентифицирует часть страницы
Cache-Control	Запрос/Ответ	Указание на то, как обрабатывать кеш
Etag	Запрос/Ответ	Тег для контента страницы
Upgrade	Запрос/Ответ	Протокол, на который хочет переключиться отправитель

АП

Артурия Пендрагон

14:38



Рис. 7.17. Кэширование HTTP

АП

Артурия Пендрагон

15:02

WAP (Wireless Application Protocol— протокол беспроводного доступа)

Артурия Пендрагон

16:43

АП трансфор–мации контента (content transformation) или транскодировании (transcoding). Он подразумевает, что компьютер, обеспечивающий связь компьютера и сервера, забирает страницу с сервера и трансформирует ее таким образом, чтобы контент подходил для мобильного устройства.

Таблица 7.15. Модули и теги XHTML Basic.

Модуль	Необходим?	Функция	Примеры тегов
Structure (Структура)	Да	Структура документа	body, head, html, title
Text (Текст)	Да	Информация	br, code, dfn, em, i, kbd, p, strong
Hypertext (Гипертекст)	Да	Гиперссылки	a
List (Списки)	Да	Списки элементов	dl, dt, dd, ol, ul, li
Forms (Формы)	Нет	Заполнение форм	form, input, label, option, textarea
Tables (Таблицы)	Нет	Прямоугольные таблицы	caption, table, td, th, tr
Image (Изображения)	Нет	Размещение изображений	img
Объект (Объекты)	Нет	Апплеты, карты и т. д.	object, param
Meta-information (Метаинформация)	Нет	Дополнительная информация	meta
Link (Ссылка)	Нет	Аналогично <a>	link
Base (База)	Нет	Точка отсчета URL	base

Google: алгоритм поиска, оценивающий, сколько раз ссылки с других страниц указывали на каждую страницу, является лучшим показателем ее важности, чем то, сколько раз на ней встречаются ключевые слова. Например, многие страницы ссылаются на главную страницу Cisco, что делает эту страницу более значимой для пользователя, который ввел «Cisco» как ключевое слово, чем страница, не относящаяся к компании, но включающая это слово много раз.

Артурия Пендрагон

17:20

АП In reply to [this message](#)

Алгоритм, который учитывал как количество, так и качество ссылок на странице, называется PageRank. Этот алгоритм был разработан Ларри Пейджем и Сергеем Брином в рамках их исследований в Стэнфордском университете и использован в поисковой системе Google для определения важности страниц в ранжировании результатов поиска. PageRank оценивает влияние страницы на основе того, сколько ссылок на нее указывают, и важности этих страниц, которые указывают на нее.

Артурия Пендрагон

20:22

АП ◆**вуковая волна** представляет собой одномерную акустическую волну (волну давления). Когда такая волна достигает уха, барабанная перепонка начинает вибрировать, вызывая вибрацию тонких костей внутреннего уха, в результате чего в мозг по нерву посыпается пульсирующий сигнал. Эта пульсация воспринимается слушателем как звук. Подобным образом, когда акустическая волна действует на микрофон, им формируется электрический сигнал, представляющий собой амплитуду звука как функцию времени.

◆**вуковые волны** можно преобразовывать в цифровую форму 20:30 при помощи аналого–цифрового преобразователя (АЦП)

При обратном процессе цифровые значения переводятся в 20:33 аналоговое электрическое напряжение. Это делается при помощи цифро–аналогового преобразователя(ЦАП)

Ошибки, возникающие в результате неточного соответствия 20:36 квантованного сигнала, способного принимать конечное число значений, исходному сигналу, называют шумом квантования (quantization noise).

Артурия Пендрагон

21:04

Для сжатия аудиофайлов было разработано множество алгоритмов. Вероятно, самые популярные форматы — это MP3 (MPEG audio layer 3 — MPEG аудио, уро-вень 3) и AAC (Advanced Audio Coding — усовершенствованное кодирование аудио), использующееся в файлах MP4 (MPEG-4)

кодировании формы сигналов (waveform coding) сигнал 21:08 раскладывается на компоненты при помощи преобразования Фурье перцепционным кодированием (perceptual coding). Она основана на некоторых недостатках слухового аппарата человека, позволяющих кодировать сигнал таким образом, что слушатель не ощутит никакой разницы по сравнению с настоящим сигналом, хотя на осциллографе эта разница будет весьма заметна. Наука, на которой базируется перцепционное кодирование, называется психоакустикой (psychoacoustics). Она изучает восприятие звука человеком. Оба формата, MP3 и AAC, используют перцепционное кодирование.

Способность громких звуков определенного диапазона 21:11 частот «прятать» более тихие звуки других диапазонов (которые были бы слышны при отсутствии громких звуков) называется частотным маскированием (frequency masking)

при появле-нии очень громкого звука коэффициент усиления 21:11 человеческого уха резко снизился, и после прекращения работы отбойных молотков требуется время на его возвращение в нормальное состояние. Этот эффект называется временным маскированием(temporal masking).

MP3 и AAC состоит в разложении сигнала в ряд Фурье для 21:19 получения силы звука на каждой из частот с последующей передачей исключительно немаскированных частот, кодируемых минимально возможным числом бит.

24 April 2023

Артурия Пендрагон

16:49

На цветном жидкокристаллическом дисплее компьютера или телевизора каждый отдельный пиксель состоит из разделенных промежутками подпикселей красного, зеленого и синего цветов. Картинки отображаются при помощи определения интенсивности подпикселей, а глаз смешивает цветовые компоненты.

Обычно картинки сменяются со скоростью 24 кадра в секунду 16:51 (так же как на 35-мм кинопленке), 30 кадров в секунду (как на американском телевидении — система NTSC) и 25 раз в секунду (как на телевизорах с системой PAL, распространенных во всем мире)

Соотношение размеров (aspect ratio) или отношение ширины 17:01 изображения в пикселях к высоте 4 : 3

Видеофайлы HDTV (High-Definition TeleVision— телевидение в 17:02 высоком разрешении) могут загружаться в разрешении 1280 на 720 пикселей. Соотношение 16 : 9\

Объем передачи = количество пикселей * битность цвета * 17:06 число кадров в секунду * длительность видео

АП

Стандарт JPEG (Joint Photographic Experts Group — объединенная группа экспертов по машинной обработке фотографических изображений) для сжатия полутоновых изображений (например, фотографий) был разработан группой экспертов,

17:12

$$\begin{aligned} Y &= 16 + 0,26R + 0,50G + 0,09B; \\ Cb &= 128 + 0,15R - 0,29G - 0,44B; \\ Cr &= 128 + 0,44R - 0,37G + 0,07B. \end{aligned}$$



Рис. 7.20. Шаги последовательного кодирования JPEG с потерями

яркости(luminance), а не к хроматическим данным (chrominance), то есть к цвету видеосигнала.

Таким образом, мы сначала вычисляем яркость, Y, и две хроматические характеристики, Cb и Cr, компонентов R, G и B.

Следующие формулы используются для 8-битных значений (от 0 до 255):

17:21

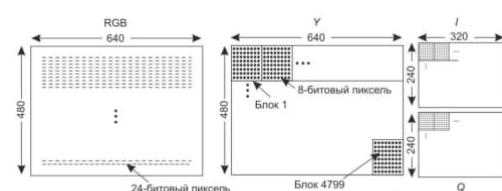


Рис. 7.21. Входные данные RGB (а). После подготовки блоков (б)

17:28

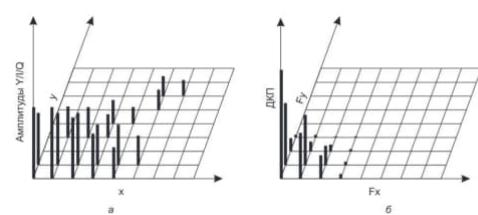


Рис 7.22. Один блок матрицы Y (а). Коэффициенты ДКП (б)

ДКП-коэффициенты								Квантованные коэффициенты							
150	80	40	14	4	2	1	0	150	80	20	4	1	0	0	0
92	75	36	10	6	1	0	0	92	75	18	3	1	0	0	0
52	38	26	8	7	4	0	0	26	19	13	2	1	0	0	0
12	8	6	4	2	1	0	0	3	2	2	1	0	0	0	0
4	3	2	0	0	0	0	0	1	0	0	0	0	0	0	0
2	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

17:31

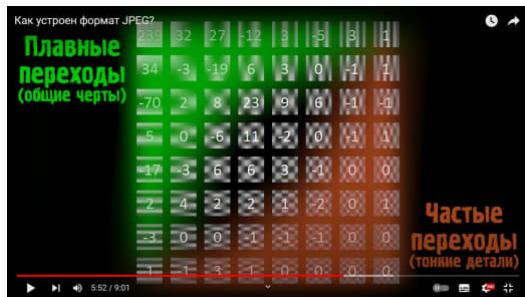
Таблица квантования							
1	1	2	4	8	16	32	64
1	1	2	4	8	16	32	64
2	2	2	4	8	16	32	64
4	4	4	4	8	16	32	64
8	8	8	8	8	16	32	64
16	16	16	16	16	16	32	64
32	32	32	32	32	32	32	64
64	64	64	64	64	64	64	64

Рис 7.23. Вычисление квантованных коэффициентов ДКП



17:34

17:43



<https://www.youtube.com/watch?v=8N0Bx8DMt6c> 17:49

<https://www.youtube.com/watch?v=z2EUT4gwkr4> 17:58

18:01

150	80	20	4	1	0	0	0
92	75	18	3	1	0	0	0
26	19	13	2	1	0	0	0
3	2	2	1	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Рис. 7.24. Порядок, в котором передаются квантованные значения.

MPEG (Motion Picture Experts Group — экспертная группа по вопросам движущегося изображения)

18:06

H.264 или AVC (Advanced Video Coding— продвинутое кодирование видео)

18:09

Артурия Пендрагон

18:27

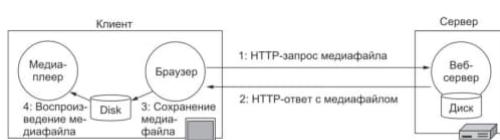
На выходе MPEG получается 3 вида кадров:

1. I- (Intracoded — закодированные в себе) кадры: содержащие сами себя сжатые не-подвижные картинки.
2. P- (Predictive — предсказательные) кадры: поблочная разница с предыдущим кадром.
3. B- (Bidirectional — двунаправленные) кадры: поблочная разница с предыдущим и последующим кадрами.

Артурия Пендрагон

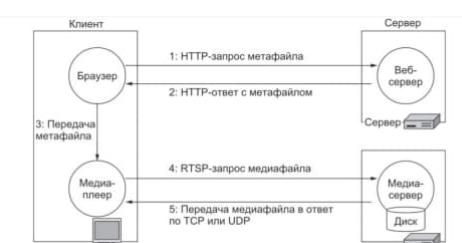
19:04

VoD (Video on Demand— видео по запросу)



19:12

Рис. 7.26. Проигрывание медиафайлов при помощи Всемирной паутины через загрузку



19:23

Рис. 7.27. Проигрывание медиафайлов при помощи Всемирной паутины и медиасервера

метафайлом (metafile) обычно очень короткий. Он включает название (и, возможно, несколько ключевых характеристик). В типичной ситуации он состоит всего лишь из одной текстовой строки, которая выглядит примерно так: `rtsp://joes-movie-server/movie-0025.mp4`

In reply to this message

19:24

RTSP (Real Time Streaming Protocol— потоковый протокол реального времени)



Рис. 7.28. Использование пакета с контролем по четности для предотвращения потерь

FEC (Forward Error Correction — заблаговременное исправление ошибок) является просто кодированием исправления ошибок

Артурия Пендрагон

20:47

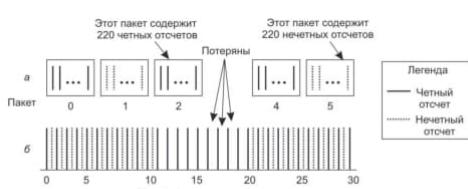


Рис. 7.29. Когда в пакетах передаются только четные или нечетные примеры, потеря пакета временно ухудшает разрешение, но не создает перерыва

интерлидингом (interleaving— чередование). Этот подход базируется на смешивании или интерлидинге порядка медиа перед передачей и сортировке или деинтерлидинге при его получении. Таким образом, благодаря перемешиванию не будет потеряно следующих друг за другом пакетов, и один большой разрыв при проигрывании медиа не образуется.

Артурия Пендрагон

21:08

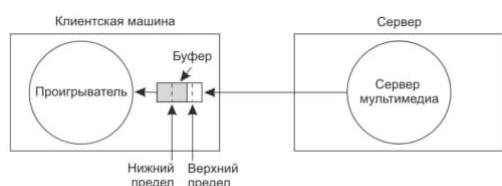


Рис. 7.30. Медиаплеер буферизует входную информацию с медиасервера и проигрывает медиа из буфера, а не напрямую из сети

Артурия Пендрагон

21:23

верхнего предела (high-water mark) сервер выдает данные лишь до тех пор, пока буфер не заполнится до верхнего предела.

Таблица 7.16. Команды RTSP, посылаемые проигрывателем на сервер

21:29

Команда	Действие сервера
DESCRIBE	Перечисляет параметры мультимедийных данных
SETUP	Устанавливает логическое соединение между проигрывателем и сервером
PLAY	Начинает отправлять данные клиенту
RECORD	Начинает прием данных от клиента
PAUSE	Приостанавливает передачу данных
TEARDOWN	Удаляет логическое соединение

firewall Межсетевой экран – фильтрует и контролирует входящий и исходящий сетевой трафик

21:35

IPTV (IP TeleVision— IP-телевидение).

21:37

25 April 2023

Артурия Пендрагон

16:35

АП

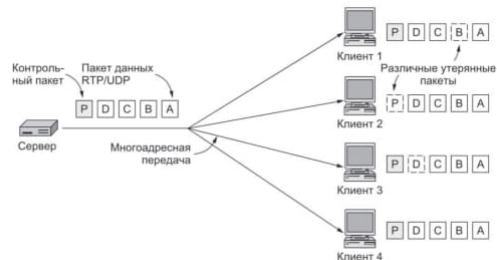


Рис. 7.31. Многоадресная передача медиа с контрольным пакетом.

АП

Артурия Пендрагон

17:01

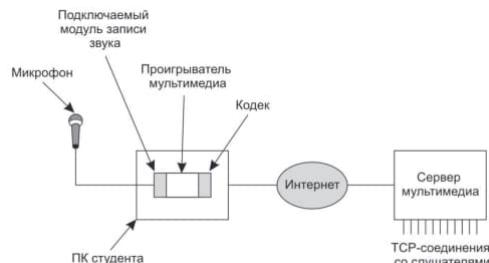


Рис. 7.32. Студенческая радиостанция

АП

Артурия Пендрагон

18:24

Международного союза телекоммуникаций (ITU)

АП

Артурия Пендрагон

18:39

Стандартное телефонное представление одного голосового канала кодируется как цифровое аудио с потоком 64 Кбит/с (8 бит на отсчет с частотой 8000 раз в секунду), что определено в G.711

установления и разрыва соединений, обеспечения тонального вызова, генерирования звуков звонков и других стандартных функций телефонной системы. Используется стандарт ITU Q.931.

Терминалам нужен протокол для ведения переговоров с машиной-приемником протокол H.225

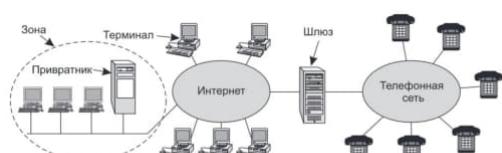


Рис. 7.33. Модель архитектуры H.323 для интернет-телефонии

18:40

шлюз (gateway) – маршрутизатор прикладного уровня (— это сетевое устройство, которое обеспечивает взаимодействие между различными протоколами и сетями на уровне приложений.)
Коммуникационные устройства называются терминалами
В локальной вычислительной сети может быть машина-привратник (gatekeeper), управляющая конечными узлами, находящимися под ее юрисдикцией (в ее зоне).

Канал между ПК и привратником, которым этот протокол управляет, называется каналом RAS (Registration/Admission/Status—Регистрация/Доступ/Статус).

18:45

18:47



Рис. 7.34. Стек протоколов H.323

рекомендации с индексом H.323 под заголовком «Видеотелефонные системы и оборудование локальных вычислительных сетей, не предоставляющих гарантированное качество обслуживания»
 ==>
 «Системы мультимедиа-коммуникаций, основанные на пакетах»

Артурия Пендрагон

19:49

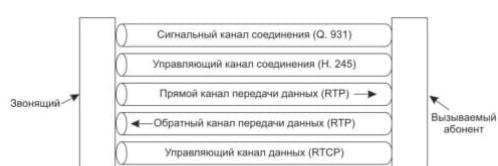


Рис. 7.35. Логические каналы между звонящим и вызываемым абонентами во время разговора

Артурия Пендрагон

20:33

системы передачи речи поверх IP — SIP (Session Initiation Protocol — протокол установления соединения)

Таблица 7.17. Методы SIP

Метод	Описание
INVITE	Запрос установления сеанса связи
ACK	Подтверждение установления сеанса
BYE	Запрос окончания сеанса
OPTIONS	Опрос возможностей хоста
CANCEL	Отмена запроса
REGISTER	Информирование сервера переадресации о текущем местоположении пользователя

20:47



Рис. 7.36. Использование прокси-сервера и переадресации в протоколе SIP

Таблица 7.18. Сравнение H.323 и SIP

Аспект	H.323	SIP
Разработчик	ITU	IETF
Совместимость с телефонной системой	Полная	В большой мере
Совместимость с Интернетом	Присутствует, по прошествии длительного времени	Присутствует
Архитектура	Монолитная	Модульная
Завершенность	Полный стек протоколов	SIP обеспечивает лишь установление соединения
Переговоры относительно параметров	Ведутся обеими сторонами	Ведутся обеими сторонами
Сигналы при вызове	Q.931 поверх TCP	SIP поверх TCP или UDP
Формат сообщений	Двоичный	ASCII
Передача мультимедийных данных	RTP/RTCP	RTP/RTCP
Многосторонняя связь	Есть	Есть
Мультимедийные конференции	Возможны	Невозможны
Адресация	URL или номер телефона	URL
Разрыв связи	Явный или разрыв TCP-соединения	Явный или по тайм-ауту

20:57

Таблица 7.18. (продолжение)

Аспект	H.323	SIP
Обмен сообщениями (instant messaging)	Нет	Есть
Шифрование данных	Есть	Есть
Объем описания стандарта	1400 страниц	250 страниц
Реализация	Громоздкая и сложная	Посредственная, но коммерчески выгодная
Статус	Широко распространена, особенно видео	Хорошая альтернатива, особенно для речи

20:57

26 April 2023

АП

Артурия Пендрагон

15:04

CDN (Content Distribution Network— сеть распределения контента). В ней поставщик рассредоточивает совокупность машин в Интернете и использует их, чтобы предоставлять контент клиентам

P2P (Peer-to-Peer — пиринговая сеть, сеть равноправных узлов). В ней совокупность компьютеров вносит свои ресурсы в общий единственный фонд, чтобы предоставлять контент друг другу, без специально установленных серверов или какого-либо центрального пункта управления

АП

Артурия Пендрагон

15:23



АП

Артурия Пендрагон

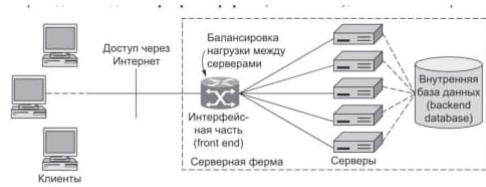
15:49

Закон Ципфа (Zipf's law) Он назван в честь Джоржа Ципфа, профессора лингвистики в Гарвардском университете, который заметил, что частота использования слова в большом тексте инверсионно пропорциональна его рангу. Например, сороковое в списке самых частотных слов используется в два раза чаще, чем восемидесятое, и в три раза чаще, чем сто двадцатое.

АП

Артурия Пендрагон

16:14



АП

Артурия Пендрагон

17:14

Веб-прокси (Web proxy) используется для того, чтобы обеспечить пользователям общий доступ к кэшу. Прокси — это агент, который действует от имени кого-то другого, например пользователя

Например, ARP-прокси отвечает на запросы ARP от имени пользователя, который находится где-то в другом месте (и не может ответить за себя). Веб-прокси выполняет веб-запросы от имени его пользователей. Он обычно обеспечивает кэширование веб-ответов, и так как он находится в совместном доступе, веб-прокси имеет существенно больший кэш, чем браузер.

17:16

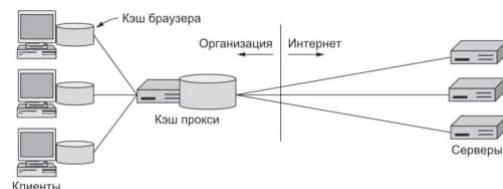


Рис. 7.39. Вспомогательный кэш между веб-браузерами и веб-серверами

Каждый браузер настроен так, что он отправляет запросы к прокси, а не к реальному серверу страницы. Если прокси имеет эту страницу, он возвращает ее немедленно. В противном случае, прокси берет страницу с сервера, добавляет ее к кэшу для будущего использования и возвращает клиенту то, что он запросил.

Артурия Пендрагон

17:48

Каждый прокси (или браузер) делает запрос к своему вышестоящему прокси (upstream proxy). Каждый вышестоящий прокси производит кэширование для нижестоящих прокси (downstream proxy) или браузеров.

CDNs (Content Delivery Networks— сети доставки контента) сам поставщик размещает копии страницы в наборе узлов в различных местах и направляет клиента, чтобы тот использовал в качестве сервера ближайший узел.

Артурия Пендрагон

18:18



Рис. 7.40. Дерево распределения CDN

Узлы в различных местах сети CDN называются зеркалами

18:23

Артурия Пендрагон

18:39

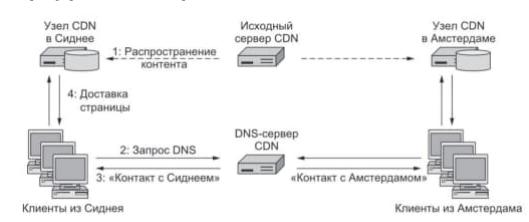


Рис. 7.41. Направление клиентов к ближайшим узлам CDN с использованием DNS

Артурия Пендрагон

18:57

Листинг 7.11. HTML-текст исходной страницы (а); та же страница после переключения на CDN (б)

```
(а)
<html>
<head> <title>Пуштостое видео</title> </head>
<body>
<h1>Список материалов Пуштостое видео</h1>
<p> Шелкните ниже на бесплатные примеры: </p>
<a href="koo1as.mp4"> Коалы сегодня </a> <br>
<a href="kangaroos.mp4"> Забавные кенгуру </a> <br>
<a href="wombats.mp4"> Милые wombats </a> <br>
</body>
</html>

(б)
<html>
<head> <title> Пуштостое видео</title> </head>
<body>
<h1>Список материалов Пуштостое видео</h1>
<p> Шелкните ниже на бесплатные примеры: </p>
<a href="http://www.cdn.com/fluffyvideo/koo1as.mp4"> Коалы сегодня </a> <br>
<a href="http://www.cdn.com/fluffyvideo/kangaroos.mp4"> Забавные кенгуру </a> <br>
<a href="http://www.cdn.com/fluffyvideo/wombats.mp4"> Милые wombats </a> <br>
</body>
</html>
```

АП

Артурия Пендрагон

15:19



- Одноранговые (пионговые) сети
- Одноранговая, децентрализованная или пионговая сеть, основанная на равноправии частников.
- Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервер, такая организация позволяет сохранить работоспособность сети при любом количестве и любом сочетании доступных узлов.



P2P (Peer-to-Peer— равноранговой сети или пионговой сети) состоит в том, что множество компьютеров вместе объединяют свои ресурсы, чтобы сформировать систему распределения контента.



**Неструктурированные
P2P - сети**

15:19



**Структурированные
P2P - сети**

15:19



Гибридные сети

15:19

BitTorrent позволить на бору узлов быстро и легко обеспечивать общий доступ к файлам

15:22

равноправных узлов (пиров)

15:23

Торрент (torrent) – это файл, содержащий метаданные, описывающие содержание, которое будет загружаться и/или распространяться через протокол BitTorrent. Этот файл-торрент содержит информацию о файле или наборе файлов, которые пользователи могут скачивать и загружать друг другу через сеть BitTorrent.

Когда пользователь хочет загрузить контент, он сначала скачивает торрент-файл, содержащий информацию о местонахождении различных частей контента и информацию о других участниках сети, которые уже загрузили или загружают этот контент. После того, как пользователь скачивает торрент-файл, его клиент BitTorrent начинает соединяться с другими клиентами в сети, чтобы начать загрузку и/или распространение контента.

In reply to [this message](#)

15:34

Торрент – это просто файл в определенном формате, который содержит два клю-чевых вида информации. Один вид называется трекер – сервер, который приводит пиринг к содержимому торрента.

Другой вид информации — список фрагментов оди-накового размера, или сегментов (chunks), из которых состоит контент.

Трекер (tracker) — это сервер, который поддерживает список всех остальных пиров, которые активно загружают и пересылают контент. Этот набор пиров называют рой (swarm)

Когда формируется начальный рой, некоторые пиры должны иметь все сегменты, составляющие контент. Эти пиры называют сидерами (seeders — сеятели— сеятели-ми).



Артурия Пендрагон

16:12

Узлы, которые берут ресурсы из системы без какого-либо вклада, называются фрирайдерами (free-riders) или личерами (leechers — пиявки).

если пир не пересыпает сегментов на другие пиры, или делает это очень медленно, рано или поздно он окажется отрезанным или заглохшим (choked)

Заглушающий алгоритм иногда описывается, как осуществление стратегии «зуб-за-зуб» (tit-for-tat)

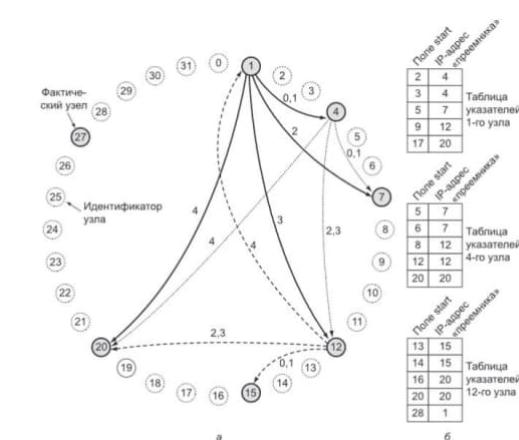
Артурия Пендрагон

16:45

DHT (Distributed Hash Tables — распределенные хэш-таблицы), поскольку основная функциональность индекса — устанавливать соответствие между ключом и значением. Это похоже на хэш-таблицу, и решения, конечно, являются распределенными версиями.

Артурия Пендрагон

17:03



28 April 2023

Артурия Пендрагон

16:24

Сообщения, подлежащие зашифровке, называемые открытым текстом (plaintext), преобразуются с помощью функции, вторым входным параметром которой является ключ (key). Результат

процесса шифрования, называемый зашифрованным текстом(ciphertext)

Искусство взлома шифров называется криптоанализом 16:25
(cryptanalysis). Искусства изобретать шифры (криптография) и взламывать их (криптоанализ) называются вместе криптологией(cryptology).



Рис. 8.1. Модель процесса шифрования—декшифрования (для шифра с симметричным ключом)

$C = EK(P)$, обозначающую, что при зашифровке открытого текста P с помощью ключа K получается зашифрованный текст C . 16:28

принцип Керкгофа гласит: Алгоритмы шифрования общедоступны; секретны только ключи. 16:34

Артурия Пендрагон 18:14

В шифрах, основанных на методе подстановки (substitution cipher), каждый символ или группа символов заменяется другим символом или группой символов.

Следующее усовершенствование состоит в установлении 18:16
соответствия каждому встречающемуся в открытом тексте символу другого символа. Например, открытый текст: a b c d e f g h i j k l m n o p q r s t u v w x y ззашифрованный текст: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M Такая система называется моноалфавитным подстановочным шифром (mono-alphabetic substitution cipher)

комбинациями из двух символов (биграммами — digrams) 18:24
являются th, in, er, re и an.

комбинациями из трех символов, или триграммами (trigrams), 18:24
являются the, ing, and и ion.

Шифры, использующие метод перестановки (transposition ciphers), меняют порядок следования символов, но не изменяют 18:30
сами символы.

M E G A B U C K		18:33
7 4 5 1 2 8 3 6		
p i e a s e t r	Открытый текст	
a n s f e r o n	please transfer on emillion dollarsto	
e m i l l i o n	myswissbankaccountsixtwotwo	
d o l l a r s t	Зашифрованный текст	
o m y s w i s s	AFLLSKSOELAWAIATOOSCTCLNMOMANT	
b a n k a c c o	ESILYNTWRNNTSOWDPAEDOBUOERIRICXB	
u n t s i x t w		
o t w o a b c d		

Рис. 8.2. Перестановочный шифр

Артурия Пендрагон 19:25

<https://ru.khanacademy.org/computing/computer-science/cryptography>

Сообщение 1:
1001001 0100001 1101100 1101111 1101110 1100101 0100000 1111001 1101111 1101010 0101110
Последовательность 1:
1010010 1001011 1100010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Зашифрованный текст:
0011011 1101011 0011110 0110100 0100100 0000110 0101011 0101001 0111000 0010011 0000101
Последовательность 2:
1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110111
Открытое сообщение 2
1000101 1101100 1101001 1100111 0100000 1101100 1101001 1101101 1100101 1110011
Рис. 8.3. Использование одноразового блокнота для шифрования сообщений и возможность получения произвольного открытого сообщения из зашифрованного путем подстановки другой ключевой последовательности

одноразовый блокнот (one-time pad) = рандом

АП

Артурия Пендрагон

19:49

квантовой криптографией

Допустим, пользователь по имени Алиса хочет передать одноразовую последовательность другому пользователю, Бобу. Алиса и Боб называются принципалами (principals).

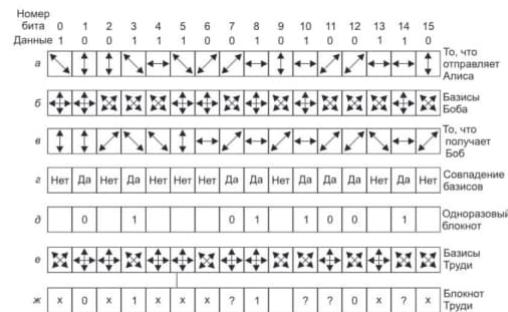
Квантовая криптография использует свойства фотонов и поляризацию света для обеспечения безопасной передачи информации. Фотоны передаются в виде квантовых битов (qubit), которые имеют два возможных состояния, например, вертикальную или горизонтальную поляризацию. Измерение состояния qubit приводит к его изменению, поэтому любая попытка перехвата информации приведет к обнаружению нарушения безопасности.

В процессе передачи информации, отправитель создает qubit с определенной поляризацией и передает его по каналу связи. Получатель использует поляризационный фильтр для измерения состояния qubit и получения информации. Если канал связи перехвачен, нарушитель изменит состояние qubit, что будет обнаружено получателем.

Поляризационные фильтры играют важную роль в квантовой криптографии, так как они позволяют управлять состоянием qubit. Их положение определяет направление поляризации света и взаимное расположение фильтров определяет угол между поляризациями.

<https://www.youtube.com/watch?v=xUch1nRpH20>

19:49



20:03

Рис. 8.4. Пример квантовой криптографии

Биты, посылаемые одним фотоном за единицу времени, называются кубитами (qubits).

АП

Артурия Пендрагон

21:08

Криптографический принцип номер 1: Сообщения должны содержать избыточные данные.

Криптографический принцип номер 2: Необходим способ борьбы с повторной от-правкой посланных ранее сообщений

АП

Артурия Пендрагон

21:42

Поляризация света – это свойство света, которое определяет направление колебаний электрического поля, связанного со светом. Если электрическое поле колеблется только в одном направлении, то свет считается поляризованным в этом направлении. Можно представить себе это как колебание на маятнике, который может двигаться только в одной плоскости. Поляризация может быть вертикальной, горизонтальной, круговой или эллиптической, в зависимости от направления и формы колебаний. Поляризационный

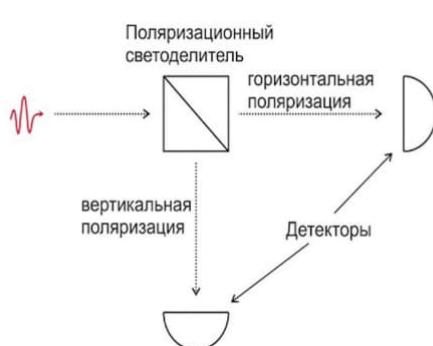
фильтр – это устройство, которое может пропускать только свет определенной поляризации, блокируя свет с другой поляризацией.

- Поляризация = направление колебаний
- Присутствует даже в отдельных фотонах. В этом случае говорят о квантовом поляризационном состоянии фотона.

Например:

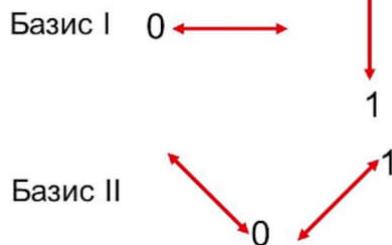
$ \leftrightarrow\rangle$	$ \updownarrow\rangle$	$ \swarrow\rangle$	$ \nwarrow\rangle$
горизонтальное	вертикальное	диагональное	антидиагональное

21:54



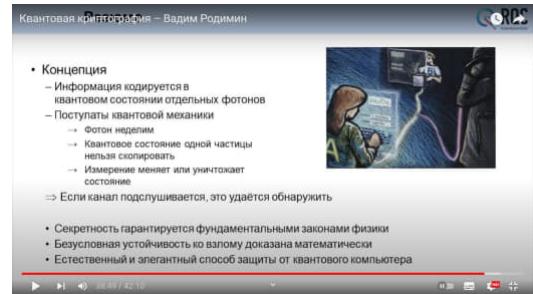
21:56

Светоделитель разделяет вертикальную и горизонтальную поляризацию. PS диагональный фoton(и антд.) 50 на 50 либо пройдет либо отразится



22:09

Чтобы сгенерировать одноразовый блокнот, Алисе понадобятся два набора поляризационных фильтров. Первый набор состоит из вертикального и горизонтального фильтров. Это называется прямолинейным базисом. Базис – это просто система координат. Второй набор фильтров отличается от первого только тем, что он повернут на 45° , то есть один фильтр можно представить в виде линии, идущей из нижнего левого угла в верхний правый, а другой – из верхнего левого в нижний правый угол. Это называется диагональным базисом



22:14

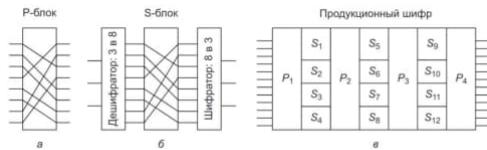
29 April 2023

Артурия Пендрагон

20:38

алго-ритмов с симметричным ключом (symmetric-key algorithms). Он получил такое название благодаря тому, что для шифрования и дешифровки сообщений применяется один и тот же ключ.

блочные шифры (block ciphers), которые принимают на входе n-битные блоки открытого текста и преобразуют их с использованием ключа в n-битный шифр.



20:43

Рис. 8.5. Основные элементы производственных шифров: Р-блок (a); С-блок (b); производственный шифр (c)

DES (Data Encryption Standard — стандарт шифрования данных) 20:58
несекретных сведений

30 April 2023

Артурия Пендрагон

12:37

In reply to [this message](#)

AES (Advanced Encryption Standard — улучшенный стандарт шифрования). Rijndael — Райн-дол основывается на теории полей Галуа

Артурия Пендрагон

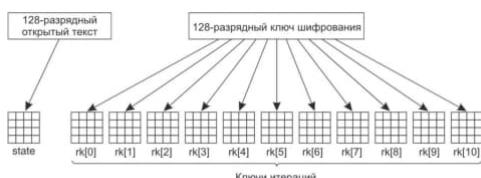
13:55

```
Листинг 8.1. Схематичный алгоритм метода Rijndael
#define LENGTH 16 /* Число байт в блоке данных или ключе */
#define NROWS 4 /* Число строк в массиве state */
#define NCOLS 4 /* Число столбцов в массиве state */
#define ROUNDS 10 /* Число итераций */
typedef unsigned char byte /* 8-разрядное целое без знака */

rijndael(byte plaintext[LENGTH], byte ciphertext[LENGTH], byte key[LENGTH])
{
    int r; /* Счетчик итерации */
    byte state[NROWS][NCOLS]; /* Текущее состояние */
    struct{byte k[NROWS][NCOLS];} rk[ROUNDS + 1]; /* Ключи итерации */

    expand_key(key, rk); /* Сформировать ключи итерации */
    copy_plaintext_to_text(state, plaintext); /* Инициализация текущего состояния */
    xor_roundkey_into_state(state, rk[0]); /* Сложить по модулю 2 ключ с текущим состоянием */

    for(r=1; r<=ROUNDS; r++) {
        substitute(state); /* Пропустить каждый байт через S-блок */
        rotate_rows(state); /* Повернуть строку 1 на 1 байт */
        if(r < ROUNDS) mix_columns(state); /* Смешивающая функция */
        xor_roundkey_into_state(state, rk[r]); /* Сложить по модулю 2 ключ с текущим состоянием */
    }
    copy_state_to_ciphertext(ciphertext, state); /* Вернуть результат */
}
```



14:09

Пример шифрования строки "HELLO" с использованием ключа "SECRETKEY":

- 1 Преобразование исходной строки в блок фиксированного размера: "HELLO" => "48454C4C4F0000000000000000000000"
- 2 Применение 10 раундов шифрования с использованием ключа "SECRETKEY".
- 3 Получение зашифрованной строки:
"20F318154B42D2AEEBA611DF743F51F"

режимом электронного шифроблокнота (Electronic Code Book mode — ECB mode),

Артурия Пендрагон

15:22

АП

Имя	Должность	Премия
А д а м с : П е с р и :	К л в р к : \$: : : : 1 0	
Б л э к : Р о б и н :	Б о с е : \$ 5 0 0 1 0 0 0	
К о л л и н з : К и м :	М в н е д ж в р : \$ 1 0 0 1 0 0 0	
Д э в и с : Б о б б и :	У б о р щ и к : \$: : : : 5	

Рис. 8.9. Открытый текст файла, зашифрованного в виде 16 DES-блоков.

In reply to this message

15:24

Выход: сцепление блоков шифра (cipher block chaining) — каждый блок открытого текста перед зашифровкой складывается по модулю 2 с предыдущим уже зашифрованным блоком. Первый блок складывается по модулю 2 со случайным вектором инициализации, IV (Initialization Vector), передаваемым вместе с зашифрованным текстом в виде открытого текста.

$$C_0 = E(P_0 \text{ XOR } IV)$$

Расшифровка производится по формуле $P_0 = IV \text{ XOR } D(C_0)$

Артурия Пендрагон

15:41

АП



Рис. 8.10. Сцепление зашифрованных блоков: а — шифрование; б — дешифрация

Артурия Пендрагон

16:00

АП

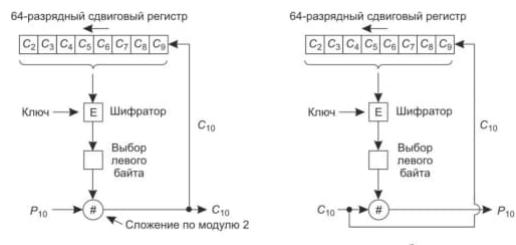


Рис. 8.11. Режим шифрованной обратной связи: а — шифрование; б — дешифрация.

Для побайтового шифрования может применяться режим шифрованной обратной связи (cipher feedback mode) с использованием (тройного) DES

Артурия Пендрагон

17:20

АП

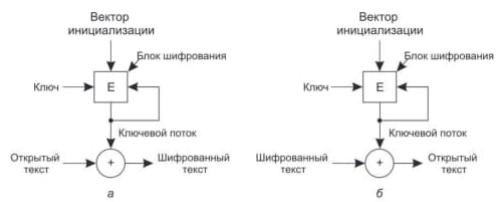


Рис. 8.12. Групповой шифр: а — шифрование; б — дешифрация

режимом группового (потокового) шифра (stream cipher mode). Суть его заключается в том, что выходной блок получается шифрованием вектора инициализации с использованием ключа. Поскольку он зависит только от вектора инициализации и ключа, ошибки передачи шифрованного текста на него не влияют.

Артурия Пендрагон

18:28

АП

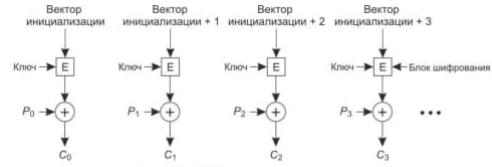


Рис. 8.13. Шифрование в режиме счетчика

режим счетчика (counter mode). Он показан на рис. 8.13. Здесь открытый текст не шифруется напрямую. Вместо этого шифруется вектор инициализации плюс некоторая константа, а уже получающийся в результате шифр складывается по модулю 2 с открытым текстом. Сдвигаясь на единицу по вектору инициализации при шифровании каждого нового блока, можно легко получить способ дешифрации любого места файла. При этом нет необходимости расшифровывать все предшествующие блоки.

Таблица 8.2. Некоторые распространенные криптографические алгоритмы с симметричными ключами

18:39

Название	Автор	Длина ключа	Комментарии
DES	IBM	56 бит	Слишком слабый для современных систем
RC4	Рональд Ривест (Ronald Rivest)	1–2048 бит	Внимание: есть слабые ключи
RC5	Рональд Ривест (Ronald Rivest)	128–256 бит	Хороший, но запатентованный
AES (Rijndael)	Домен (Daemen) и Раймен (Rijmen)	128–256 бит	Лучший
Serpent	Андерсон (Anderson), Байхам (Baihram) и Кнауден (Knudsen)	128–256 бит	Очень сильный
Тройной DES	IBM	168 бит	Хороший, но устаревает
Twofish	Брюс Шнайер (Bruce Schneier)	128–256 бит	Очень сильный; широко распространен

RC4 (Rivest Cipher 4) – это поточный алгоритм шифрования, который использует ключевую последовательность для шифрования данных. Принцип работы RC4 заключается в генерации псевдослучайной последовательности на основе ключа и комбинации этой последовательности с данными, которые нужно зашифровать.

RC5 (Rivest Cipher 5) – это блочный алгоритм шифрования, который использует переменный размер блока и ключа. Принцип работы RC5 заключается в повторении операций замены и перестановки для каждого блока данных, используя ключ и вектор инициализации.

Serpent – это блочный алгоритм шифрования, который использует 128-битные блоки и ключи длиной от 128 до 256 бит. Принцип работы Serpent основан на применении повторяющихся раундов замены, перестановки и XOR.

Тройной DES (Triple DES) – это симметричный блочный алгоритм шифрования, который использует 64-битные блоки и 168-битный ключ. Принцип работы Тройного DES заключается в том, что каждый блок данных проходит через три различных операций DES с тремя различными ключами.

Twofish – это блочный алгоритм шифрования, который использует 128-битные блоки и ключи длиной от 128 до 256 бит. Принцип работы Twofish основан на применении нелинейных операций замены и линейных перестановок для каждого раунда шифрования.

Артурия Пендрагон

19:10

АП
криptoанализ:

дифференциальным криptoанализом (Biha и Shamir, 1997). Он может использоваться для взлома любых блочных шифров. Теория вероятности линейным криptoанализом С его помощью можно взломать DES только с 243 известными открытыми текстовыми блоками. Принцип

работы основан на суммировании по модулю 2 некоторых бит открытого текста и изучении результатов для шаблонных последовательностей.

Анализ энергосбережения. Если криптографический алгоритм состоит из цикла, в котором разряды ключа обрабатываются поочередно, взломщик, заменив главный системный п-гигагерцовый тактовый генератор медленным (например, с частотой 100 Гц) и повесив «крокодилы» на ножки питания и заземления центрального процессора, может с большой точностью отслеживать мощность, потребляемую каждой машинной инструкцией.

Анализ времени. Криптографические алгоритмы содержат большое количество условных операторов (if), тестирующих биты итерационных ключей. Если части then и else выполняются за различное время, то, замедлив системный тактовый генератор и измерив длительность всех шагов, можно вычислить ключи итераций. По этим ключам обычно можно вычислить и общий ключ.

Артурия Пендрагон

21:48

RSA (Rivest, Shamir, Adleman). Теория чисел. 1. Выберем два больших простых числа p и q (обычно длиной 1024 бита). 2. Сосчитаем $n = p \times q$ и $z = (p-1) \times (q-1)$. 3. Выберем число d , являющееся взаимно простым с числом z . 4. Найдем такое число e , что остаток от деления произведения $e \times d$ на число z равен 1. $C = P^e \pmod{n}$ $P = C^d \pmod{n}$

Открытый текст (P)		Зашифрованный текст (C)		После дешифрации	
Символ	Число	P^3	$P^3 \pmod{33}$	C^7	$C^7 \pmod{33}$
S	19	6859	28	13492928512	19
U	21	9261	21	1801088541	21
Z	26	17576	20	1280000000	26
A	01	1	1	1	1
N	14	2744	5	78125	14
N	14	2744	5	78125	14
E	05	125	26	8031810176	5

Вычисление отправителя

Вычисление получателя

21:57

Рис. 8.14. Пример работы алгоритма RSA

$p = 3$, а $q = 11$, что дает значения $n = 33$, а $z = 20$. Число d можно выбрать равным 7, так как числа 20 и 7 не имеют общих делителей. При таком выборе значение e можно найти, решив уравнение $7e \equiv 1 \pmod{20}$, откуда следует, что $e = 3$. Шифрованный текст C получается из открытого сообщения P по формуле $C = P^3 \pmod{33}$. Получатель расшифровывает сообщение по формуле $P = C^7 \pmod{33}$

Первым алгоритмом с открытым ключом стал «алгоритм ранца» (Merkle и Hellman, 1978). Его идея состоит в том, что имеется большое количество объектов различного веса. Владелец этих объектов кодирует сообщение, выбирая подмножество объектов и помещая их в ранец. Общий вес объектов в рюкзаке известен всем, как и список всех возможных объектов и их соответствующий вес. Список объектов, находящихся в рюкзаке, хранится в секрете. При определенных дополнительных ограничениях задача определения возможного списка объектов по известному общему весу считалась неразрешимой по вычислениям, то есть считалось, что решение можно найти только полным перебором различных сочетаний предметов списка. Поэтому она была положена в основу алгоритма с открытым ключом.

1 May 2023

Артурия Пендрагон

17:25

АП

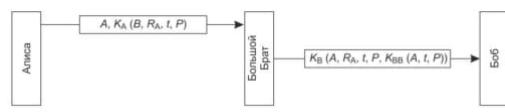


Рис. 8.15. Цифровая подпись Большого Брата

сообщение Р, она формирует сообщение, зашифрованное КА (ключом Алисы), КА(В, RA, t, P), где В— идентификатор Боба, RA— случайное число, выбранное Алисой, t— временной штамп, подтверждающий свежесть сообщения.

Сообщение, посылаемое Бобу, содержит открытый текст сообщения Алисы и подпись Большого Брата КВВ(А, t, Р).

Артурия Пендрагон

17:53

АП

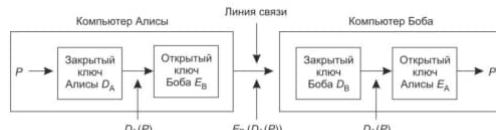


Рис. 8.16. Цифровая подпись, полученная при помощи шифрования с открытым ключом

Стандарта цифровой подписи DSS (Digital Signature Standard) 18:06
вариант алгоритма с открытым ключом Эль-Гамаля на сложности вычисления дискретных логарифмов

Эта схема основана на идее необратимой хэш-функции, 18:15
которая принимает на входе участок открытого текста
произвольной длины и по нему вычисляет строку битов
фиксированной длины. У этой хэш-функции, часто называемой
профилем сообщения(message digest, MD),

Артурия Пендрагон

18:47

АП



Рис. 8.17. Цифровая подпись с использованием профиля сообщения

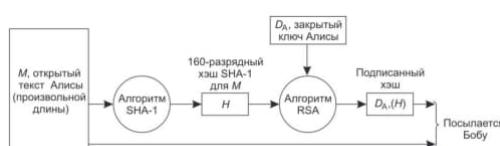


Рис. 8.18. Применение SHA-1 и RSA для создания подписей несекретных сообщений

Артурия Пендрагон

19:14

АП



Рис. 8.19. Сообщение, дополненное до размера, кратного 512 битам (a); выходные переменные (б); массив слов (в)

SHA-1 (Secure Hash Algorithm 1) является хэш-функцией, которая преобразует произвольное сообщение в 160-битный хэш-код. Она использует серию логических операций для разбиения сообщения на блоки, которые затем обрабатываются и объединяются, чтобы получить конечный хэш-код. SHA-1 также включает дополнительные шаги, такие как добавление битовых строк и контрольную сумму, для повышения безопасности.

MD5(MessageDigest 5 — профиль сообщения 5) Сначала 19:26
сообщение дополняется до длины 448 бит по модулю 512. Затем к

нему добавляется исходная длина сообщения, рассматриваемая как 64-разрядное число, в результате чего получается блок битов длиной кратной 512. Последний шаг подготовки к вычислениям инициализирует 128-разрядный буфер, задавая его содержимое равным некоему фиксированному значению. Далее начинаются вычисления. На каждом этапе берется 512-разрядный блок входного текста и тщательно перемешивается со 128-разрядным буфером. Для пущей наваристости в кастрюлю также кидается содержимое таблицы синусов

Артурия Пендрагон

19:55

АП

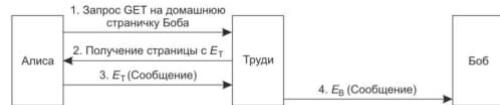


Рис. 8.20. Способ вторжения в систему с открытыми ключами

Артурия Пендрагон

21:09

АП

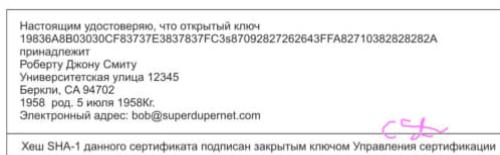


Рис. 8.21. Пример сертификата и подписанных хэшов

Артурия Пендрагон

21:59

АП

Таблица 8.3. Основные поля сертификата в стандарте X.509

Поле	Значение
Version	Версия X.509
Serial number	Это число вместе с названием Управления сертификации однозначно идентифицирует сертификат
Signature algorithm	Алгоритм генерации подписи сертификата
Issuer	X.500-имя Управления
Validity period	Начало и конец периода годности
Subject name	Сущность, ключ которой сертифицируется
Public key	Открытый ключ сущности и идентификатор использующего его алгоритма
Issuer ID	Необязательный идентификатор, единственным образом определяющий эмитента (создателя) сертификата
Subject ID	Необязательный идентификатор, единственным образом определяющий владельца сертификата
Extensions	Различные возможные расширения
Signature	Подпись сертификата (генерируется с помощью закрытого ключа Управления сертификации)

2 May 2023

Артурия Пендрагон

16:45

АП

альтернативный способ сертификации открытых ключей. Он известен под общим названием PKI (Public Key Infrastructure — инфраструктура систем с открытыми ключами)

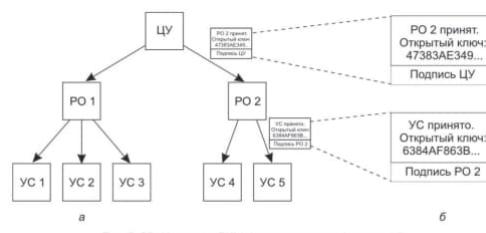


Рис. 8.22. Иерархия PKI (а); цепочка сертификатов (б)

Управление сертификации верхнего уровня (root) мы будем называть Центральным управлением (ЦУ). Центральное управление сертифицирует управление второго уровня — назовем их Региональными отделами (РО — Regional Authorities, RA), — так как они могут обслуживать некоторый географический регион, например страну или континент. Региональные отделы, в свою очередь, занимаются легализацией реальных Управлений

сертификации (УС), эмитирующих сертификаты стандарта X.509 для физических и юридических лиц.

Артурия Пендрагон

17:39

IPsec(IP security— IP-безопасность) на сетевом уровне

Артурия Пендрагон

18:00

Технически IPsec состоит из двух основных частей. Первая описывает два новых заголовка, которые можно добавлять к пакету для передачи идентификатора защиты, данных контроля целостности и другой информации. Вторая часть, ISAKMP(Internet Security and Key Management Protocol— интернет-безопасность и протокол управления ключами), предназначена для создания ключей. ISAKMP является средой. Основным протоколом для выполнения работы является IKE (Internet Key Exchange — обмен ключами в Интернете).



18:09

Рис. 8.23. Заголовок идентификации IPsec в транспортном режиме для IPv4

вычислении хэш-функции для пакета и общего ключа.

18:16

Отдельно общий ключ, конечно, не передается. Подобная схема называется HMAC (Hashed Message Authentication Code — код идентификации хэшированного сообщения)



18:18

Рис. 8.24. ESP: а — в транспортном режиме; б — ESP в режиме туннелирования

Альтернативой заголовку IPsec служит заголовок ESP (Encapsulating Security Payload— инкапсулированная защищенная полезная нагрузка)

Артурия Пендрагон

19:49

АП

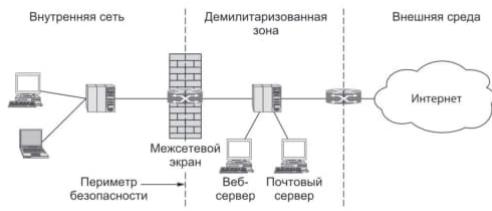


Рис. 8.25. Межсетевой экран, защищающий внутреннюю сеть

867Межсетевые экраны (firewalls, также называемые брандмауэрами) представляют собой современную реализацию средневекового принципа обеспечения безопасности. Они напоминают ров, вырытый вокруг замка. Суть конструкции заключается в том, что все входящие и выходящие из замка должны проходить по одному подъемному мосту, где полиция ввода/вывода сможет проверить их личность. Тот же принцип может быть применен и в сетях: у компании может быть несколько локальных сетей, соединенных произвольным образом, но весь внешний трафик должен проходить через электронный подъемный мост (межсетевой экран), как показано на рис. 8.25. Не существует никакого другого пути.

Брандмауэр работает как пакетный фильтр (packet filter) 19:50

In reply to [this message](#) 19:54

DMZ (DeMilitarized Zone— демилитаризированная зона) это часть сети компании, которая не угрожает ее безопасности. Сюда включается все. Если разместить веб-сервер в DMZ, то компьютеры через Интернет могут войти с ним в контакт, чтобы зайти на сайт компании.

Артурия Пендрагон 20:50

АП

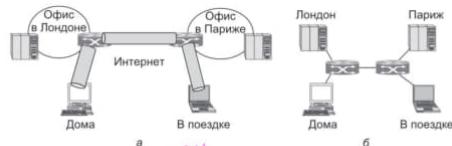


Рис. 8.26. а. Виртуальная частная сеть. б. Топология, видимая изнутри сети

3 May 2023

Артурия Пендрагон 16:48

WPA2 (WiFi Protected Access 2— защищенный доступ к WiFi, версия 2). Часть стандарта 802.11, называемая 802.11i, описывает протокол безопасности канального уровня, не позволяющий беспроводному узлу читать или другим образом вмешиваться в сообщения, посланные другой парой беспроводных узлов.

EAP (Extendable Authentication Protocol — расширенный протокол аутентификации) (RFC 3748), который описывает, как взаимодействуют клиент и аутентификационный сервер. EAP является средой, а другие стандарты определяют сообщения протокола.

Сообщение от клиента защищено проверкой целостности, которая называется MIC (Message Integrity Check — проверка целостности сообщения), данная проверка основывается на ключе сеанса.

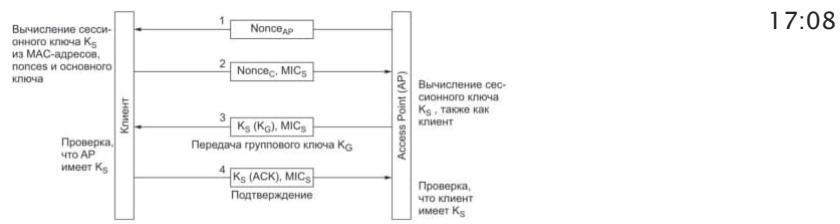


Рис. 8.27. Четырехпакетное опознавание и генерация сеансового ключа в 802.11i

Артурия Пендрагон 17:38

TKIP (Temporary Key Integrity Protocol — временный протокол целостности ключа) — новый версион CCMP? Это сокращение от Counter mode with Cipher block chainin message authentication code protocol — режим счетчика с протоколом аутентификации в режиме сцепления обратной связи.

Артурия Пендрагон 19:23

1. Действительно ли это процесс Скотта (аутентификация)? 2. Имеет ли Скотт право удалять файл cookbook.old (авторизация)?

Центром распространения ключей (KDC— Key Distribution Center) 19:24

19:29

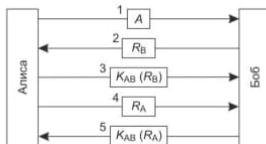


Рис. 8.28. Двусторонняя аутентификация при помощи протокола оклик-ответ

одна сторона посылает другой случайное число, которое другая сторона преобразует особым образом и возвращает результат. Такие протоколы называются протоколами типа оклик-ответ (challenge-response)

In reply to this message

19:30

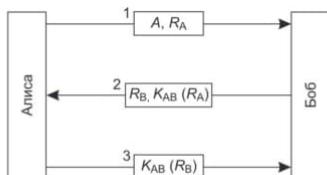


Рис. 8.29. Укороченный двусторонний протокол аутентификации

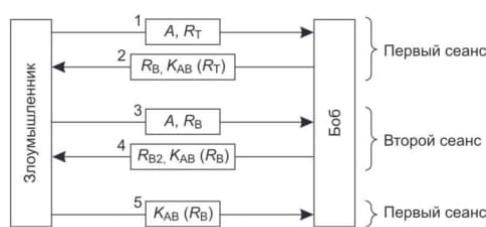


Рис. 8.30. Зеркальная атака

зеркальная атака (reflection attack). В частности, Труди может взломать его, если ей будет позволено одновременно открыть несколько сеансов связи с Бобом. Такое вполне возможно, если, скажем, Боб — это банк, позволяющий устанавливать несколько одновременных соединений с банкоматами.

Артурия Пендрагон

20:24

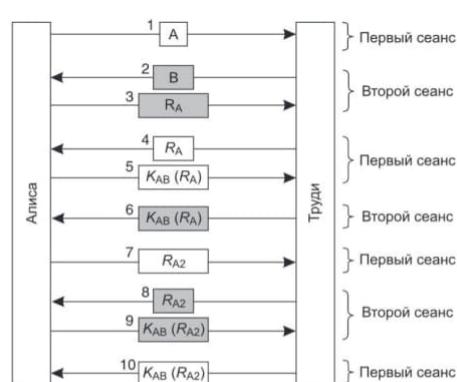


Рис. 8.31. Зеркальная атака протокола, показанного на рис. 8.28

In reply to this message

20:28

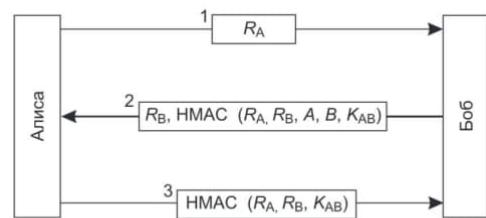


Рис. 8.32. Аутентификация с применением HMAC

20:35

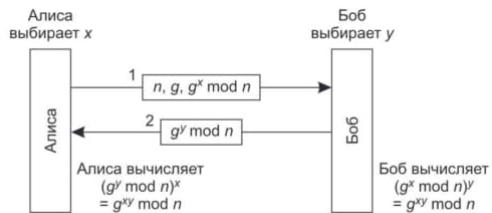


Рис. 8.33. Протокол обмена ключами Диффи—Хеллмана

Протокол, позволяющий не встречавшимся ранее людям устанавливать общий се-кремтный ключ, называется протоколом обмена ключами Диффи—Хеллмана (Diffie—Hellman key exchange). Для примера возьмем (совершенно нереальные) значения $n=47$ и $g=3$. Алиса выбирает значение $x=8$, а Боб выбирает $y=10$. Оба эти числа хранятся в секрете. Со—10. Оба эти числа хранятся в секрете. Со—10. Оба эти числа хранятся в секрете. Сообщение Алисы Бобу содержит числа (47, 3, 28), так как $38 \bmod 47 = 28$. Боб отвечает Алисе числом 17. Алиса вычисляет $178 \bmod 47$ и получает 4. Боб вычисляет $2810 \bmod 47$ и получает также 4. Таким образом, независимо друг от друга, Алиса и Боб определили, что значение секретного ключа равно 4. Чтобы найти ключ, злоумышленнику придется решить уравнение $3x \bmod 47 = 28$, что можно сделать путем полного перебора для таких небольших чисел, но только не для чисел длиной в несколько сотен бит.

In reply to this message

20:36



Рис. 8.34. Атака типа «человек посередине»

«пожарная цепочка» (bucket brigade attack), поскольку слегка напоминает старинных пожарных, передававших друг другу по цепочке ведра с водой.

4 May 2023

Артурия Пендрагон

16:06

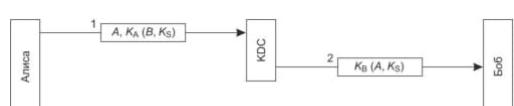


Рис. 8.35. Первая попытка протокола аутентификации с помощью KDC-центра

Идея, лежащая в основе протокола, проста: Алиса выбирает ключ сеанса, K_S , и заявляет KDC, что она желает поговорить с Бобом при помощи ключа K_S .

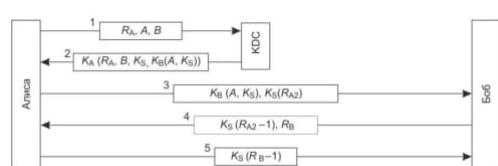


Рис. 8.36. Протокол аутентификации Нидхэма—Шредера

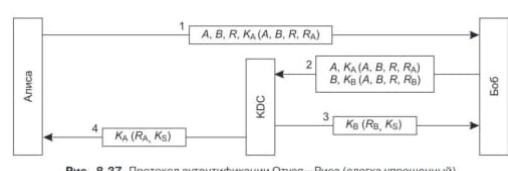


Рис. 8.37. Протокол аутентификации Отзуя—Риса (слегка упрощенный)

Артурия Пендрагон

16:56

АП

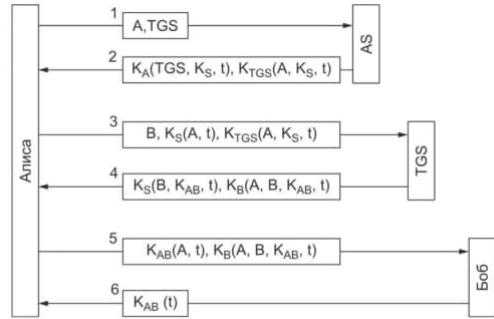


Рис. 8.38. Работа протокола Kerberos V5

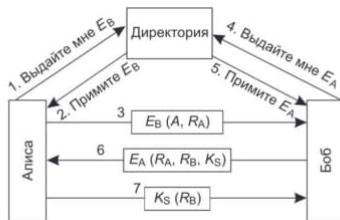


Рис. 8.39. Взаимная идентификация с помощью открытого ключа

17:11

Артурия Пендрагон

19:13

АП

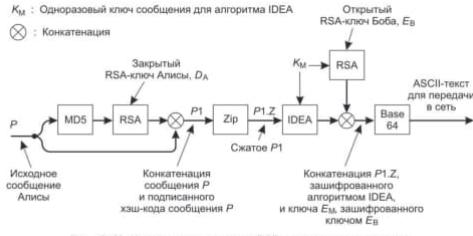


Рис. 8.40. Использование системы PGP для передачи сообщения

PGP (Pretty Good Privacy) — довольно хорошая конфиденциальность
Циммерман является сторонником безопасности в сетях и его девиз таков: «Если конфиденциальность нарушается, значит, она доступна только нарушителям закона». PGP кодирует данные с помощью блочного шифра IDEA (International Data Encryption Algorithm) — международный алгоритм шифрования данных), используя ключи длиной 128 бит.

19:20



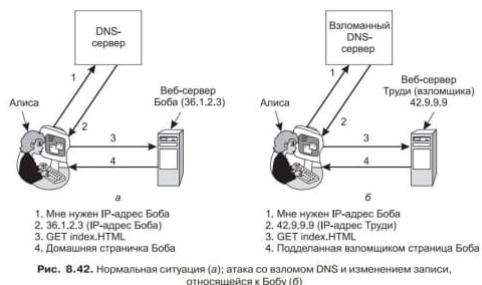
S/MIME (Secure/MIME — защищенный MIME) До тех пор пока сертификат может быть проверен по доверительному якорю, он считается корректным

5 May 2023

Артурия Пендрагон

17:37

АП



Вправа 77. Запишіть подані іменники разом або через дефіс.
 1. Земле/черепашка, місто/зінходження, закон/творчість, лієо/стен,
 20/річка, п'яглескти/річка, перво/зісанник, електро/шнур, віце/прем'єр, су-
 пер/зірка, авто/дорога, учитель/фізик, хімік/біолог, красуня/дівчина, рі-
 ка/Десна, Іваненко/сон, Петро/молотий, спориш/трава, ягода/малина, худо-
 жник/пейзажист, хірург/лікар, українка/дівчина, співачка/лівів'янка, запо-
 рожжка/місто, Дінпро/ріка, Леонов/космонавт, актор/Леонов, гуси/лебеді,
 хліб/сіль, землемістрий, жаро/міцність, вербо/ліз, пів/Донецька, напів/автомат,
 напів/европеєць, високо/новажний, жук/рогач, ліон/довгунець, сту-
 дент/практикант, електро/кардіограф, стол/крин, чар/зілля, свят/вечір, джер-
 ело/знавець, історик/археолог, дівчина/голубка, член/кореспондент,
 еко/членів, лже/патріот, лже/Путачов, анти/фашист, генерал/лейтенант, мі-
 ні/футбол, мікро/елемент, макро/економіка, контр/адмірал, контр/удар.
 2. Вантаж/і/потік, житте/лікс, звір/зів, кості/грав, час/різка, но-
 во/будова, лісо/смуга, гучно/мовесь, дизель/мотор, генерал/майор, всюди/хід,
 радіо/комітет, секундо/мір, тепло/ноз, шляко/блок, вело/спорт, теле/передача,
 держ/стандарт, кино/фільм, телефон/автомат, танц/майданчик, лісо/стен,
 міськ/рада, місце/хід, магазин/салон, ліон/довгунець, полін/трава,
 авіа/десант, авто/фургон. *Іванчик*.

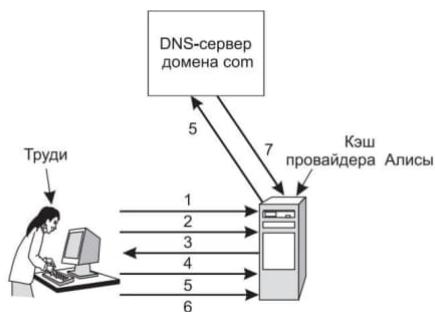
Вправа 78. Запишіть подані іменники разом або через дефіс.

АП

Артурия Пендрагон

17:37

21:05



In reply to this message

21:05

Во-перших, провайдер Алиси
все-таки проверяет наличие в ответе правильного адреса сервера
верхнего уровня.

Но Труди может написать в соответствующем поле что угодно и преодолеть эту преграду. Учитывая то, что адреса серверов верхнего уровня общедоступны, сделать это несложно.

Во-вторых, для того чтобы DNS-сервер мог понять, какому запросу соответствует

ответ, во все запросы добавляются порядковые номера. Чтобы обмануть провайдера

Алисы, Труди должна знать текущий порядковый номер. Самый простой способ узнать его — это зарегистрировать собственный домен, например trudy-the-intruder.com.

Предположим, что IP-адрес этого домена также **42.9.9.9**. Труди создает DNS-сервер

для этого домена: dns.trudy-the-intruder.com. Его IP-адрес тот же самый (**42.9.9.9**),

поскольку оба домена расположены на одном и том же компьютере.

Теперь надо заставить провайдера Алисы поинтересоваться DNS-сервером Труди. Сделать это несложно. Требуется лишь запросить,

например, foobar.trudy-the-intruder.com, и серверу

проводайдера Алисы придется опросить сервер верхнего уровня, .com, и узнать у него,

кто обслуживает новый домен Труди.
И вот теперь, когда запись <dns.trudy-the-intruder.com> занесена в кэш провайдера, можно спокойно начинать атаку. Труди запрашивает у провайдера Алисы <www>.
<trudy-the-intruder.com>, а тот в ответ посылает на DNS-сервер Труди соответствующий запрос. Вот в этом-то запросе и содержится нужный злоумышленнице порядковый номер. Теперь Труди должна действовать без промедления: она ищет с помощью провайдера Алисы Боба и тут же отвечает на собственный вопрос, посылая фальшивку:
«Адрес <bob.com>: 42.9.9.9». Этот подделанный ответ несет в себе порядковый номер, на единицу больше только что полученного. За время атаки она может послать еще одну фальшивку, с номером, на два больше полученного, а также еще около дюжины таких «ответов» с увеличивающимися номерами. Задача одного из них нам уже ясна.
Остальные никому не нужны, их просто выкинут. После прибытия фальшивого ответа на запрос Алисы он будет помещен в кэш; к тому времени, когда доберется настоящий ответ, он будет отвергнут, так как сервер уже ничего не ожидает

[Артурия Пендрагон](#)

21:24

DNSsec предоставляет три основные услуги.

1. Подтверждение места отправления данных.
2. Распространение открытых ключей.
3. Аутентификацию транзакций и запросов.'

Записи DNS группируются в наборы, называемые RRSet
(Resource Record)

21:25

Set — набор записей ресурсов). В набор входят все записи с одинаковыми именами, классами и типами. Скажем, в наборе может быть несколько записей A, если имя DNS соответствует первичному и вторичному IP-адресам

Таблица 8.4. Пример набора RRSet для bob.com. Запись KEY содержит открытый ключ Боба. Запись SIG — это хэш A и KEY, подписанный сервером домена верхнего уровня (.com) для проверки их аутентичности

21:35

Имя домена	Время жизни	Класс	Тип	Значение
bob.com.	86400	IN	A	36.1.2.3
bob.com.	86400	IN	KEY	3682793A7873F731029CE2737D...
bob.com.	86400	IN	SIG	86947503A88848F5272E53930C...

типа записей — SIG. В такой записи содержится подписанный хэш, сформированный в соответствии с алгоритмом, указанным в KEY

6 May 2023

[Артурия Пендрагон](#)

18:25

SSL (Secure Sockets Layer — протокол защищенных сокетов) М

Итак, SSL создает защищенное соединение между двумя сокетами, позволяющее: 1) клиенту и серверу договориться об используемых параметрах; 2) провести аутентификацию сервера клиентом; 3) организовать тайное общение; 4) обеспечить защиту целостности данных.

Если поверх SSL используется HTTP, этот вариант называется 18:25 HTTPS (Secure HTTP — защищенный HTTP)

18:29



Рис. 8.44. Уровни (и протоколы), используемые обычным домашним браузером с SSL.

Артурия Пендрагон

19:14

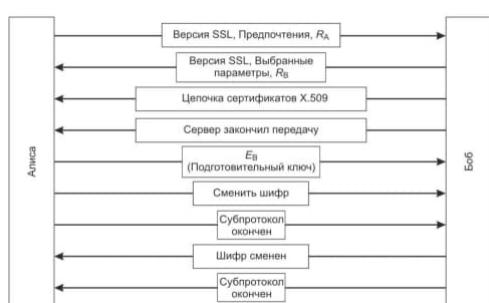


Рис. 8.45. Упрощенный вариант субпротокола SSL установления соединения



Хэш добавляется к каждому фрагменту в виде MAC (Message Authentication Code — код аутентификации сообщения)

направила SSL на стандартизацию в IETF. Результатом стал 19:24 стандарт TLS (Transport Layer Security— защита транспортного уровня)

НОНС (Nonce) в криптографии обычно используется в 19:25 контексте протоколов аутентификации и шифрования, где он служит для генерации случайного числа или значения, которое может использоваться только один раз.]

Артурия Пендрагон

19:45

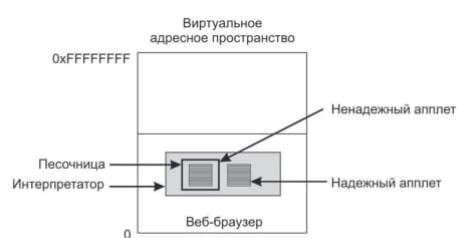


Рис. 8.47. Апплеты могут интерпретироваться веб-браузером

Java-апплеты — это небольшие программы на языке Java, откомпилированные в ма-апплеты — это небольшие программы на языке Java, откомпилированные в ма-Java, откомпилированные в ма-, откомпилированные в ма-шаблонный язык со стековой организацией под названием JVM (Java Virtual Machine— виртуальная машина Java). Если же апплет не может считаться надежным (например, он был загружен из Интернета), его можно поместить в так называемую песочницу(sandbox), регулирующую его поведение и пресекающую его попытки использовать системные ресурсы.

АП

Артурия Пендрагон

20:55

Так же как в веб-страницы можно добавить код, точно так же можно сделать дополнение к браузерам (browser extension — расширение браузера; add-on — дополнение к браузеру, «аддон»; plug-in — подключаемый модуль, «плагин»), и рынок этих дополнений растет. Эти дополнения представляют собой компьютерные программы, которые расширяют функциональность веб-браузеров.

7 May 2023

АП

Артурия Пендрагон

11:53

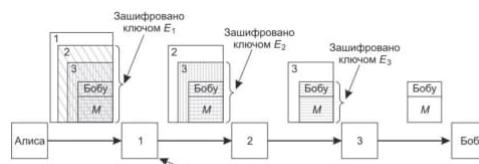
Уильям Тиндэйл (William Tyndale) был английским богословом и лингвистом, который родился в 1494 году в графстве Глостершир. Он стал известен как первый человек, который перевел Библию на английский язык.

В то время Библия была доступна только на латынице и греческом языках, и только священники и другие ученые могли ее прочесть. Тиндэйл решил перевести Библию на английский, чтобы обычные люди могли ее читать и понимать. Он начал свою работу над переводом в 1520 году, в то время как учился в Оксфорде и Кембридже.

Однако его работа была неодобрена церковными властями того времени. Перевод Библии на английский язык был считался еретическим, так как церковь считала, что обычные люди не могут правильно понимать Священное Писание без помощи священников.

Тиндэйл был вынужден покинуть Англию и продолжить свою работу в Европе, где он работал над переводом Библии на английский язык и издавал книги с переводом на немецкий и другие европейские языки. Его переводы Библии были широко распространены, и он стал национальным героем для многих англичан.

Однако, Тиндэйл был выслежен церковными властями, и в 1535 году он был арестован в городе Антверпен в Бельгии. Он был приговорен к смерти по обвинению в ереси и 6 октября 1536 года был сожжен на костре. Его последними словами были: "Господи, открай глаза короля на английский народ".



12:05

Рис. 8.48. Использование трех анонимных рассылок для передачи письма Алисы Бобу

АП

Артурия Пендрагон

12:43

Итого, ip-адрес имеет стратегическое значение, указывая, куда глобально надо передать пакет, тас же имеет тактическое значение, в нём содержится информация, какому ближайшему устройству (из нашей же сети) нужно передать информацию.

АП

Артурия Пендрагон

14:11

Ценное замечание высказывает Джон Гилмор (John Gilmore): «Сеть воспринимает цензуру как разрушенный участок дороги и идет в

обход». Конкретная реализация этой мысли называется службой вечности (eternity service) (Anderson, 1996). Ее цель — гарантировать, что однажды опубликованные материалы не исчезнут и не будут переписаны заново, как было принято в Советском Союзе во времена Сталина. Пользователь службы вечности должен лишь указать, в течение какого срока следует обеспечивать сохранность информации, заплатить пропорциональную сроку и объемам информации сумму и загрузить данные на сервер. После этого никто, включая самого пользователя, не сможет удалить или отредактировать размещенные на сервере службы вечности материалы.

Как такую услугу реализовать на практике? Проще всего организовать равноранговую (пири ngовую) систему, в которой документы будут размещаться на десятках серверов участников проекта, каждый из которых будет получать свою долю вознаграждения, что послужит стимулом для их вступления в проект. Серверы должны располагаться в самых разных местах и под разной юрисдикцией, что обеспечит максимальную устойчивость системы. Списки 10 выбранных случайным образом серверов следует хранить в тайне в разных местах, чтобы в случае неудачи, произошедшей с одним из них, могли выжить другие. Любые государственные органы, помешанные на уничтожении неугодной информации, никогда не смогут быть до конца уверенными в том, что они нашли все копии. Кроме того, систему можно сделать самовосстанавливающейся, в том смысле, что в случае прихода известия об уничтожении каких-то экземпляров документов, держатели остальных копий попытаются найти новые места хранения на замену выбывшим из строя.

Служба вечности была первой попыткой противостояния цензуре в Сети.

Люди, которым требуется секретное общение, зачастую пытаются скрыть сам факт общения. Наука, занимающаяся скрытием сообщений, называется стеганографией (steganography), от греческого слова, которое можно перевести как «защищенное письмо»

14:13