Оглавление

[Тема 1. Введение. Обзорные лекции 2](#_Toc517198296)

[Лекция 1.1 Структура глобальной телекоммуникационной сети ЭВМ. Классификации и топологии сетей. Вводные понятия. 2](#_Toc517198297)

[ТЕМА 2. Модели ВОС (OSI) и TCP/IP 7](#_Toc517198298)

[Лекция 2.1 Модель взаимодействия открытых систем (OSI). Протоколы.Изучение сети. Сетевые протоколы и сетевой доступ. Модели OSI и TCP/IP 7](#_Toc517198299)

[**Лекция 2.2 Стек TCP/IP. Инкапсуляция данных. Примеры протоколов** 17](#_Toc517198300)

[ТЕМА 3. Физические среды передачи данных. Виды подключений 21](#_Toc517198301)

[Лекция 3.1 Медный кабель: STP, UTP, коаксиальный кабель 21](#_Toc517198302)

[Лекция 3.2 Оптическая и беспроводная среда передачи данных. Антенны 23](#_Toc517198303)

[Тема 4. IP-адресация. Разбиение сетей на подсети 30](#_Toc517198304)

[Лекция 4.1 Адреса IPv4 30](#_Toc517198305)

[Лекция 4.2 Адреса IPv6 32](#_Toc517198306)

[Лекция 4.3 Статическая и динамическая адресация. Маска подсети IPv4. NAT 34](#_Toc517198307)

[Тема 5. Основы телекоммуникационных сетей 42](#_Toc517198308)

[Лекция 5.1 Аналоговые и цифровые сигналы. АЦП и ЦАП. Спектр сигналов 42](#_Toc517198309)

[Лекция 5.2 Основы шифрования данных 46](#_Toc517198310)

[Лекция 5.3 Помехоустойчивое кодирование данных 50](#_Toc517198311)

[Лекция 5.4 Методы цифровой модуляции сигналов 55](#_Toc517198312)

[Тема 6. Беспроводные телекоммуникационные сети. WLAN-сети. Проектирование сетей Wi-Fi 59](#_Toc517198313)

[Лекция 6.1 Wi-Fi. Методы высокоскоростной передачи данных. OFDM и MIMO 59](#_Toc517198314)

[Лекция 6.2 Особенности проектирования радиопокрытия локальных беспроводных сетей Wi-Fi (WLAN) 63](#_Toc517198315)

[Лекция 6.3 Основные понятия мобильных телекоммуникаций. Основы сетей 2G (GSM) 68](#_Toc517198316)

[**Лекция 6.4 Основы сетей 3G (WCDMA)** 71](#_Toc517198317)

[Лекция 6.5 Основы сетей 4G (LTE, LTE-Advanced) 73](#_Toc517198318)

# Тема 1. Введение. Обзорные лекции

## Лекция 1.1 Структура глобальной телекоммуникационной сети ЭВМ. Классификации и топологии сетей. Вводные понятия.

**Структура глобальной телекоммуникационной сети ЭВМ представлена на рисунке 1.**

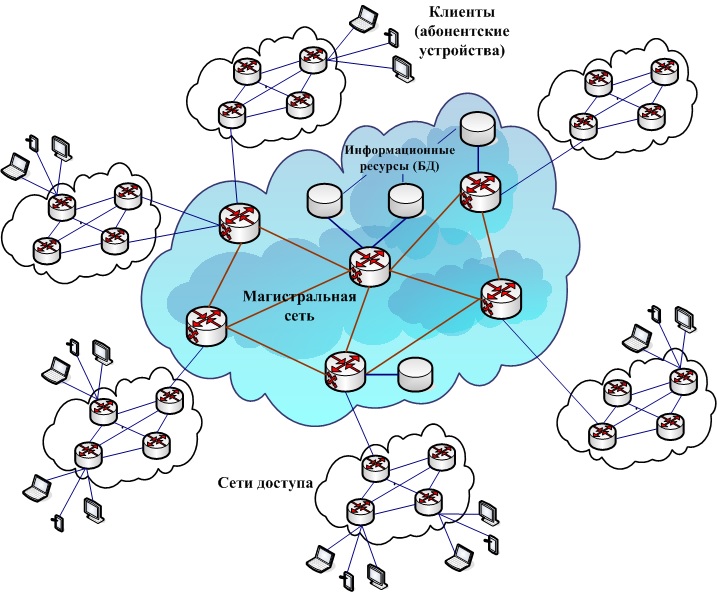


Рисунок 1 - структура телекоммуникационной сети ЭВМ

**Функционирование сети** осуществляется следующим образом:

Сообщение формируется прикладной пользовательской программой и отправляется в сеть. СПД доставляет сообщение компьютеру по адресу, указанному в заголовке, и соответствующему ПП (прикладному процессу). Если ПП-отправитель направил запрос ПП - базе данных, то последний сформирует ответ на полученный запрос. Сетевое ПО добавит к полученному сообщению-ответу необходимые для передачи атрибуты и отправит процессу-отправителю. На этом цикл обмена сообщениями заканчивается, он носит название сессии.

**Основные понятия**

***Сети ЭВМ –***совокупность средств вычислительной техники, представляющих собой множество ЭВМ, объединенных с помощью средств телекоммуникаций. Основные функции сетей ЭВМ – это обработка и передача данных.

***ЭВМ (электронная вычислительная машина, компьютер) –***совокупность технических средств, предназначенных для организации ввода, хранения, обработке с помощью различного рода программного обеспечения и вывода данных.

К техническим средствам можно отнести: центральный процессор, оперативная память, внешние устройства, устройства ввода-вывода информации, различные запоминающие устройства

***Сеть ЭВМ***- это совокупность компьютеров, коммутационно-распределительного оборудования, объединенных каналами связи, и программного обеспечения.

Основные функции сетей ЭВМ:

·         это обработка и передача данных

·          обеспечение коллективного использования аппаратных и информационных ресурсов ЭВМ.

·         Создание АСУ различных типов.

·         Создание распределенных баз данных и организация удаленного доступа пользователей к ним с ЭВМ сети.

**Функции ЭВМ, включенных в сеть:**

1) Сервера - предоставление своих ресурсов удаленным пользователям.

2) Клиенты или рабочие станции - потребители сервиса, предоставляемого машинами-серверами.

**Классификация сетей ЭВМ**

 1. По размеру (по территориальному охвату):

• Персональные (Personal Area Network - PAN) – Bluetooth, ZigBee

• Локальные (Local Area Network - LAN) – Ethernet, Token Ring, Wi-Fi (IEEE802.11)

• Городские, региональные (Metropolitan Area Network - MAN) – IEEE802.16 (WiMAX), LTE, GSM

• Глобальные (Wide Area Network - WAN) – базируются на технологиях Frame Relay, X25, TCP/IP, ATM, и т.д.

2. По принадлежности:

• Офисные

• Корпоративные

• Частные (Virtual Private Network - VPN)

•

3. По назначению:

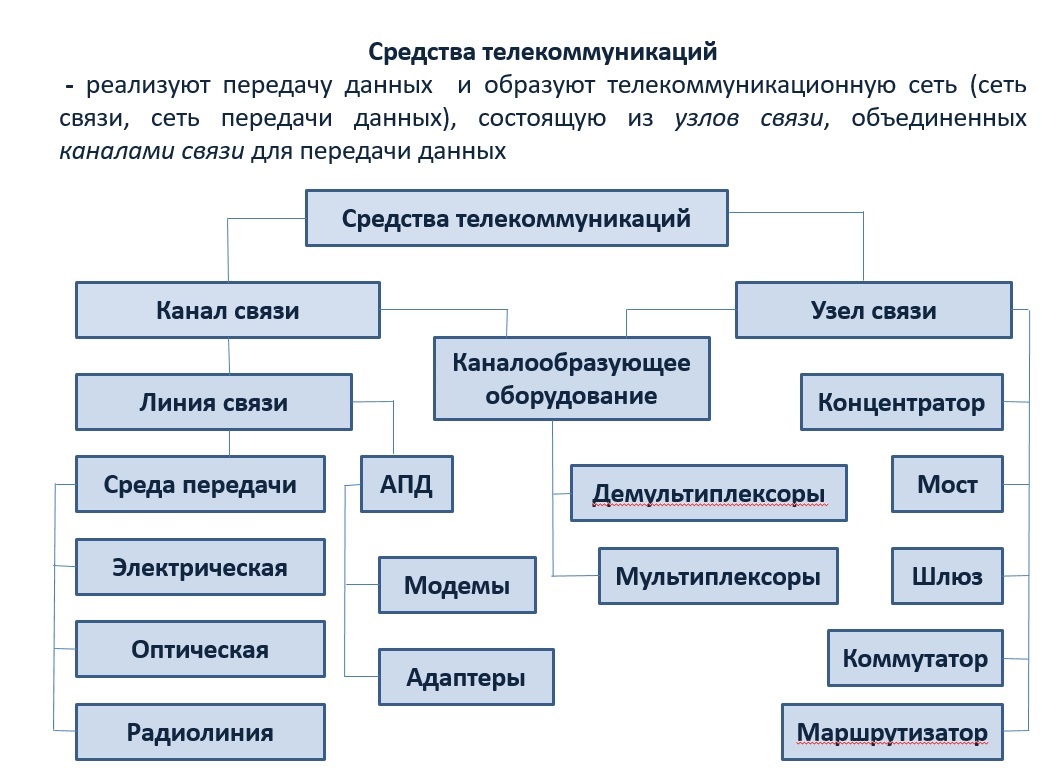
• Вычислительные

• Информационные

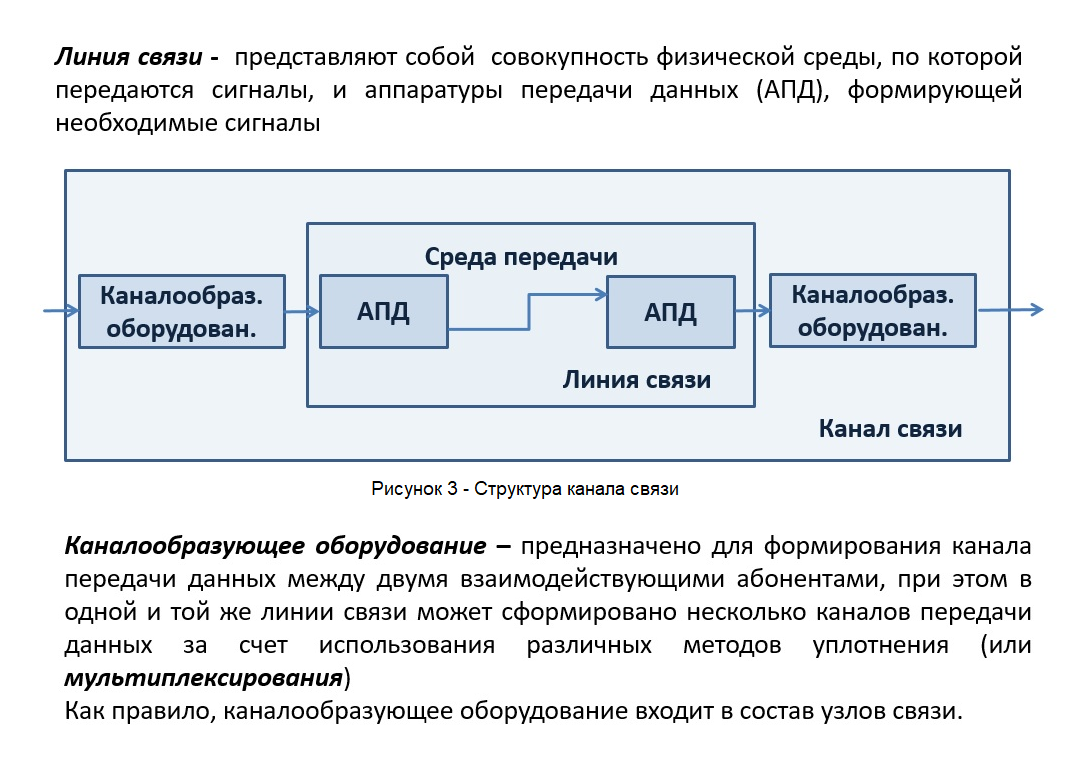
• Информационно-вычислительные

• Информационно-управляющие

На рисунках 2 и 3 показаны средства коммуникацийэ



**Рисунок 2 – Классификация средств телекоммуникаций**

****

**Основные функции узлов связи:**

• Маршрутизация – выбор направления (маршрута) передачи данных в сетях связи

• Коммутация – установление физического или логического соединения абонентов коммуникационной сети через транзитные узлы

• Мультиплексирование - уплотнение канала, т. е. передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу. В телекоммуникациях мультиплексирование подразумевает передачу данных по нескольким логическим каналам связи в одном физическом канале. В информационных технологиях мультиплексирование подразумевает объединение нескольких потоков данных (виртуальных каналов) в один.

• Демультиплексирование – разделение одного входящего в узел связи потока данных на несколько выходящих из узла потоков

**Принципы структурной организации компьютерных сетей. Сетевые топологии**

**Общая шина** – представляет собой кабель, называемый шиной или магистралью, к которому подсоединены компьютерные сети. Выход из строя шины приведет к полному отказу сети (рисунок4).



Рисунок 4 – Топология сети «Общая шина»

**Дерево** – формируется по принципу «минимума суммарной длины связей между узлами сети» и является основой для построения иерархических сетей. В таких сетях существует только один путь  между двумя любыми узлами, что делает задачу маршрутизации тривиальной (рисунок5).

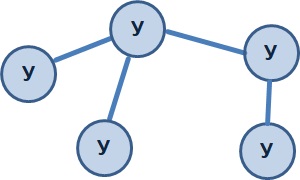


Рисунок 5 – Топология сети «Дерево»

**Звезда** – содержит один центральный узел, к которому присоединяются все остальные узлы сети. В качестве центрального узла может выступать мощный компьютер, который может предоставлять свои ресурсы периферийным компьютерам и выполнять функции маршрутизатора, либо сетевые устройства (коммутатор или концентратор) (рисунок6).

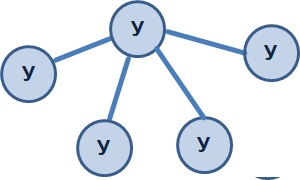


Рисунок 6 – Топология сети «Звезда»

**Кольцо** – каждый узел связан с двумя другими узлами. Основное достоинство топологии- наличие альтернативного маршрута в случае разрыва линии (рисунок7).

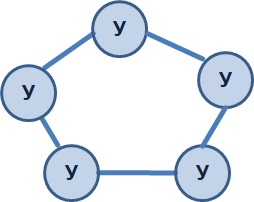


Рисунок 7 – Топология сети «Кольцо»

**Полносвязная** – формируется по принципу каждый с каждым. Такая топология наиболее эффективна по всем основным показателям качества функционирования – надежности, производительности и пр. Однако, стоимость запредельна (рисунок8).

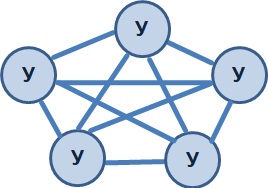


Рисунок 8 – Топология сети «Полносвязная»

**Многосвязная (или ячеистая)**– формируется по принципу «каждый узел должен быть соединен не менее чем с двумя соседним узлами» для наличия хотя бы одного альтернативного маршрута в случае отказа какого-либо участка сети (рисунок9).

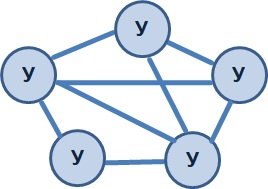


Рисунок 9 – Топология сети «Многосвязная»

**Смешанная топология** – представляет собой комбинацию рассмотренных выше топологий и обычно образуется при объединении нескольких локальных сетей (рисунок 10).

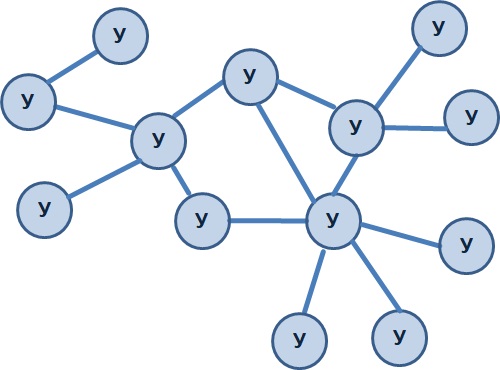


Рисунок 10 – Топология сети «Смешанная»

# ТЕМА 2. Модели ВОС (OSI) и TCP/IP

## Лекция 2.1 Модель взаимодействия открытых систем (OSI). Протоколы.Изучение сети. Сетевые протоколы и сетевой доступ. Модели OSI и TCP/IP



Рисунок 11 – Модель OSI

На рисунке 11 представлена модель OSI. А рисунок 12 показывает сравнение моделей OSI и TCP/IP

**Протоколы физического уровня** описывают электрические, механические, функциональные и процедурные средства для активации, поддержки и деактивации физического соединения, обеспечивающего передачу битов из одного сетевого устройства в другое.

·         **Протоколы канального уровня** описывают способы обмена кадрами данных при обмене данными между устройствами по общей среде передачи данных.

·         **Сетевой уровень** предоставляет функции для обмена отдельными частями данных по сети между указанными оконечными устройствами.

·         **Транспортный уровень** определяет сервисы для сегментации, передачи и сборки данных для отдельных коммуникаций между оконечными устройствами.

·         **Сеансовый уровень** передает сервисы на уровень представления для организации его диалога и управления обмена данными.

·         **Уровень представления** обеспечивает общее представление данных, передаваемых между службами прикладного уровня.

·         **Прикладной уровень** содержит протоколы для обмена данными между процессами.

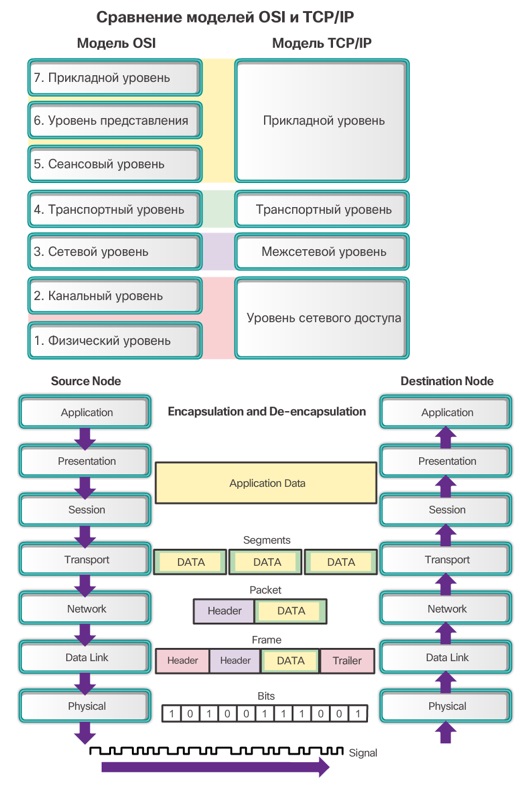


Рисунок 12 – Сравнение моделей OSI и TCP/IP

**Прикладной уровень (Application layer)**

Прикладной уровень обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам.

прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты.

 В модели OSI прикладная программа, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере), посылает конкретные данные в виде Дейтаграммы на прикладной уровень. Одна из основных задач этого уровня – определить, как следует обрабатывать запрос прикладной программы, другими словами, какой вид должен принять данный запрос.

Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (messege).

Прикладной уровень выполняет следующие функции:

1.       Выполнение различных видов работ.

-         передача файлов;

-         управление заданиями;

-         управление системой и т. д;

2.       Идентификация пользователей по их паролям, адресам, электронным подписям;

3.       Определение функционирующих абонентов и возможности доступа к новым прикладным процессам;

4.       Определение достаточности имеющихся ресурсов;

5.       Организация запросов на соединение с другими прикладными процессами;

6.       Передача заявок представительскому уровню на необходимые методы описания информации;

7.       Выбор процедур планируемого диалога процессов;

8.       Управление данными, которыми обмениваются прикладные процессы и синхронизация взаимодействия прикладных процессов;

9.       Определение качества обслуживания (время доставки блоков данных, допустимой частоты ошибок);

10.   Соглашение об исправлении ошибок и определении достоверности данных;

11.   Согласование ограничений, накладываемых на синтаксис (наборы символов, структура данных).

Указанные функции определяют виды сервиса, которые прикладной уровень предоставляет прикладным процессам. Кроме этого, прикладной уровень передает прикладным процессам сервис, предоставляемый физическим, канальным, сетевым, транспортным, сеансовым и представительским уровнями.

**На прикладном уровне** необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское программное обеспечение.

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу **наиболее распространенных протоколов верхних трех уровней** относятся:

-  FTP (File Transfer Protocol) протокол передачи файлов;

-  TFTP (Trivial File Transfer Protocol) простейший протокол пересылки файлов;

-  X.400 электронная почта;

-  Telnet работа с удаленным терминалом;

-  SMTP (Simple Mail Transfer Protocol) простой протокол почтового обмена;

-  CMIP (Common Management Information Protocol) общий протокол управления информацией;

-  SLIP (Serial Line IP) IP для последовательных линий. Протокол последовательной посимвольной передачи данных;

-  SNMP (Simple Network Management Protocol) простой протокол сетевого управления;

-  FTAM (File Transfer, Access, and Management) протокол передачи, доступа и управления файлами.

**Уровень представления данных (Presentation layer)**

Функции данного уровня – представление данных, передаваемых между прикладными процессами, в нужной форме.

Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе. В случаях необходимости уровень представления в момент передачи информации выполняет преобразование форматов данных в некоторый общий формат представления, а в момент приема, соответственно, выполняет обратное преобразование. Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. Такая ситуация может возникнуть в ЛВС с неоднотипными компьютерами (IBM PC и Macintosh), которым необходимо обмениваться данными. Так, в полях баз данных информация должна быть представлена в виде букв и цифр, а зачастую и в виде графического изображения. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой.

В основу общего представления данных положена единая для всех уровней модели система ASN.1. Эта система служит для описания структуры файлов, а также позволяет решить проблему шифрования данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня.

**Представительный уровень** выполняет следующие основные функции:

1.       Генерация запросов на установление сеансов взаимодействия прикладных процессов.

2.       Согласование представления данных между прикладными процессами.

3.       Реализация форм представления данных.

4.       Представление графического материала (чертежей, рисунков, схем).

5.       Засекречивание данных.

6.       Передача запросов на прекращение сеансов.

Протоколы уровня представления данных обычно являются составной частью протоколов трех верхних уровней модели.

**Сеансовый уровень (Session layer)**

Сеансовый уровень – это уровень, определяющий процедуру проведения сеансов между пользователями или прикладными процессами.

Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент, а также предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того чтобы начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

**Сеансовый уровень управляет** передачей информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. Функции этого уровня состоят в координации связи между двумя прикладными программами, работающими на разных рабочих станциях. Это происходит в виде хорошо структурированного диалога. В число этих функций входит создание сеанса, управление передачей и приемом пакетов сообщений во время сеанса и завершение сеанса.

**На сеансовом уровне** определяется, какой будет передача между двумя прикладными процессами:

-  полудуплексной (процессы будут передавать и принимать данные по очереди);

-  дуплексной (процессы будут передавать данные, и принимать их одновременно).

В полудуплексном режиме сеансовый уровень выдает тому процессу, который начинает передачу, маркер данных. Когда второму процессу приходит время отвечать, маркер данных передается ему. Сеансовый уровень разрешает передачу только той стороне, которая обладает маркером данных.

**Сеансовый уровень обеспечивает** выполнение следующих функций:

1.    Установление и завершение на сеансовом уровне соединения между взаимодействующими системами.

2.    Выполнение нормального и срочного обмена данными между прикладными процессами.

3.    Управление взаимодействием прикладных процессов.

4.    Синхронизация сеансовых соединений.

5.    Извещение прикладных процессов об исключительных ситуациях.

6.    Установление в прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки.

7.    Прерывание в нужных случаях прикладного процесса и его корректное возобновление.

8.    Прекращение сеанса без потери данных.

9.    Передача особых сообщений о ходе проведения сеанса.

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью протоколов трех верхних уровней модели.

**Транспортный уровень (Transport Layer)**

Транспортный уровень предназначен для передачи пакетов через коммуникационную сеть. На транспортном уровне пакеты разбиваются на блоки.

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Транспортный уровень определяет адресацию физических устройств (систем, их частей) в сети. Этот уровень гарантирует доставку блоков информации адресатам и управляет этой доставкой. Его главной задачей является обеспечение эффективных, удобных и надежных форм передачи информации между системами. Когда в процессе обработки находится более одного пакета, транспортный уровень контролирует очередность прохождения пакетов. Если проходит дубликат принятого ранее сообщения, то данный уровень опознает это и игнорирует сообщение.

**В функции транспортного уровня** входят:

1.       Управление передачей по сети и обеспечение целостности блоков данных.

2.       Обнаружение ошибок, частичная их ликвидация и сообщение о неисправленных ошибках.

3.       Восстановление передачи после отказов и неисправностей.

4.       Укрупнение или разделение блоков данных.

5.       Предоставление приоритетов при передаче блоков (нормальная или срочная).

6.       Подтверждение передачи.

7.       Ликвидация блоков при тупиковых ситуациях в сети.

Начиная с транспортного уровня, все вышележащие протоколы реализуются программными средствами, обычно включаемыми в состав сетевой операционной системы.

Наиболее распространенные протоколы транспортного уровня включают в себя:

-  TCP (Transmission Control Protocol) протокол управления передачей стека TCP/IP;

-  UDP (User Datagram Protocol) пользовательский протокол дейтаграмм стека TCP/IP;

-  NCP (NetWare Core Protocol) базовый протокол сетей NetWare;

-  SPX (Sequenced Packet eXchange) упорядоченный обмен пакетами стека Novell;

-  TP4 (Transmission Protocol) – протокол передачи класса 4.

**Сетевой уровень (Network Layer)**

Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор маршрута наиболее быстрого и надежного пути.

Сетевой уровень устанавливает связь в вычислительной сети между двумя системами и обеспечивает прокладку виртуальных каналов между ними. Виртуальный или логический канал – это такое функционирование компонентов сети, которое создает взаимодействующим компонентам иллюзию прокладки между ними нужного тракта. Кроме этого, сетевой уровень сообщает транспортному уровню о появляющихся ошибках. Сообщения сетевого уровня принято называть пакетами (packet). В них помещаются фрагменты данных. Сетевой уровень отвечает за их адресацию и доставку.

Прокладка наилучшего пути для передачи данных называется маршрутизацией, и ее решение является главной задачей сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.

Протокол канального уровня обеспечивает доставку данных между любыми узлами только в сети с соответствующей типовой топологией. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами.

Таким образом, внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень. При организации доставки пакетов на сетевом уровне используется понятие номер сети. В этом случае адрес получателя состоит из номера сети и номера компьютера в этой сети.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Для того чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач (hops) между сетями, каждый раз, выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет.

Сетевой уровень отвечает за деление пользователей на группы и маршрутизацию пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

**Сетевой уровень выполняет** функции:

1.       Создание сетевых соединений и идентификация их портов.

2.       Обнаружение и исправление ошибок, возникающих при передаче через коммуникационную сеть.

3.       Управление потоками пакетов.

4.       Организация (упорядочение) последовательностей пакетов.

5.       Маршрутизация и коммутация.

6.       Сегментирование и объединение пакетов.

**На сетевом уровне определяется** два вида протоколов. Первый вид относится к определению правил передачи пакетов с данными конечных узлов от узла к маршрутизатору и между маршрутизаторами. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений.

Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

**Наиболее часто на сетевом уровне** используются протоколы:

-  IP (Internet Protocol) протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию;

-  IPX (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell;

-  X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2);

-  CLNP (Connection Less Network Protocol) сетевой протокол без организации соединений.

**Канальный уровень (Data Link)**

Единицей информации канального уровня являются кадры (frame). Кадры – это логически организованная структура, в которую можно помещать данные. Задача канального уровня – передавать кадры от сетевого уровня к физическому уровню.

На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок.

**Канальный уровень обеспечивает** корректность передачи каждого кадра, помещая специальную последовательность бит, в начало и конец каждого кадра, чтобы отметить его, а также вычисляет контрольную сумму, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка.

Задача канального уровня – брать пакеты, поступающие с сетевого уровня и готовить их к передаче, укладывая в кадр соответствующего размера. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать ошибки передачи.

На этом же уровне определяются правила использования физического уровня узлами сети. Электрическое представление данных в ЛВС (биты данных, методы кодирования данных и маркеры) распознаются на этом и только на этом уровне. Здесь обнаруживаются и исправляются (путем требований повторной передачи данных) ошибки.

**Канальный уровень обеспечивает** создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. Спецификации IEEE 802.Х делят канальный уровень на два подуровня:

-  LLC (Logical Link Control) управление логическим каналом осуществляет логический контроль связи. Подуровень LLC обеспечивает обслуживание сетевого уровня и связан с передачей и приемом пользовательских сообщений.

-  MAC (Media Assess Control) контроль доступа к среде. Подуровень MAC регулирует доступ к разделяемой физической среде (передача маркера или обнаружение коллизий, или столкновений) и управляет доступом к каналу связи. Подуровень LLC находится выше подуровня МАC.

**Канальный уровень определяет** доступ к среде и управление передачей посредством процедуры передачи данных по каналу.

При больших размерах передаваемых блоков данных канальный уровень делит их на кадры и передает кадры в виде последовательностей.

При получении кадров уровень формирует из них переданные блоки данных. Размер блока данных зависит от способа передачи, качества канала, по которому он передается.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

**Канальный уровень может выполнять** следующие виды функций:

1.       Организация (установление, управление, расторжение) канальных соединений и идентификация их портов.

2.       Организация и передача кадров.

3.       Обнаружение и исправление ошибок.

4.       Управление потоками данных.

5.       Обеспечение прозрачности логических каналов (передачи по ним данных, закодированных любым способом).

Наиболее часто используемые протоколы на канальном уровне включают:

-  HDLC (High Level Data Link Control) протокол управления каналом передачи данных высокого уровня, для последовательных соединений;

-  IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x;

-  Ethernet сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей частоты и обнаружением конфликтов;

-  Token ring сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера;

-  FDDI (Fiber Distributed Date Interface Station) сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;

-  X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов;

-  Frame relay сеть, организованная из технологий Х25 и ISDN.

**Физический уровень (Physical Layer)**

**Физический уровень предназначен** для сопряжения с физическими средствами соединения. Физические средства соединения – это совокупность физической среды, аппаратных и программных средств, обеспечивающая передачу сигналов между системами.

Физическая среда – это материальная субстанция, через которую осуществляется передача сигналов. Физическая среда является основой, на которой строятся физические средства соединения. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц.

Физический уровень состоит из Подуровня стыковки со средой и Подуровня преобразования передачи.

Первый из них обеспечивает сопряжение потока данных с используемым физическим каналом связи. Второй осуществляет преобразования, связанные с применяемыми протоколами. Физический уровень обеспечивает физический интерфейс с каналом передачи данных, а также описывает процедуры передачи сигналов в канал и получения их из канала. На этом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел. Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

-  тип кабелей и разъемов;

-  разводку контактов в разъемах;

-  схему кодирования сигналов для значений 0 и 1.

Физический уровень выполняет следующие функции:

1.  Установление и разъединение физических соединений.

2.  Передача сигналов в последовательном коде и прием.

3.  Прослушивание, в нужных случаях, каналов.

4.  Идентификация каналов.

5.  Оповещение о появлении неисправностей и отказов.

Оповещение о появлении неисправностей и отказов связано с тем, что на физическом уровне происходит обнаружение определенного класса событий, мешающих нормальной работе сети (столкновение кадров, посланных сразу несколькими системами, обрыв канала, отключение питания, потеря механического контакта и т.д.). Виды сервиса, предоставляемого канальному уровню, определяются протоколами физического уровня. Прослушивание канала необходимо в тех случаях, когда к одному каналу подключается группа систем, но одновременно передавать сигналы разрешается только одной из них. Поэтому прослушивание канала позволяет определить, свободен ли он для передачи. В ряде случаев для более четкого определения структуры физический уровень разбивается на несколько подуровней.

**Лекция 2.2 Стек TCP/IP. Инкапсуляция данных. Примеры протоколов**

Для успешного обмена данными между узлами связи существует набор сетевых протоколов, описывающий правила их взаимодействия. Сетевые протоколы определяют общий формат и набор правил для обмена сообщениями между устройствами.

Задачи сетевых протоколов:

·                   определение способа форматирования и структурирования сообщений;

·                   организация процесса обмена информацией, связанной с маршрутизацией, между сетевыми устройствами;

·                   описание способов и времени передачи сообщений об ошибках, а формирование также системных сообщений между устройствами;

·                   установление и завершение сеансов передачи данных.

Стек протоколов – это группа протоколов, используемых для предоставления комплексных сетевых сервисов. Стеки протоколов формализуются организациями по стандартизации или производителями сетевого оборудования.

**Стек протоколов TCP/IP**

TCP/IP (Transmission Control Protocol/Internet Protocol) – это стандарт стека протоколов, разработанный для глобальных сетей Интернет, публикующийся серией документов, названных RFC (Request for Comment). На рисунке 13 показана структура и примеры протоколов стека TCP/IP, а также выполнено сопоставление с уровнями модели OS (рисунок 13).

Уровень доступа к сети – самый нижний уровень стека, который по факту не определяется стандартом, но поддерживает взаимодействие с такими протоколами (технологиями) как:

·                   Ethernet – технология, определяющая правила для прокладки кабелей и обмена сигналами на уровне сетевого доступа, описываемая стандартами IEEE группы 802.3;

·                   RS232 – стандарт физического уровня, известный как последовательный порт для персональных ЭВМ;

·                   GSM – стандарт 2-ого поколения мобильной связи, описывающий процедуры уровня сетевого доступа (или физического и канального уровня модели OSI);

·                   UMTS – стандарт 3-ого поколения мобильной связи, описывающий процедуры уровня сетевого доступа (или физического и канального уровня модели OSI);

·                   LTE – стандарт 4-ого поколения мобильной связи, описывающий процедуры уровня сетевого доступа (или физического и канального уровня модели OSI);

·                   PPP – технология, предоставляющая средства инкапсуляции пакетов для передачи через последовательный канал;

·                   Wi-Fi (IEEE 802.16) – набор стандартов связи для передачи данных в беспроводных локальных сетях.

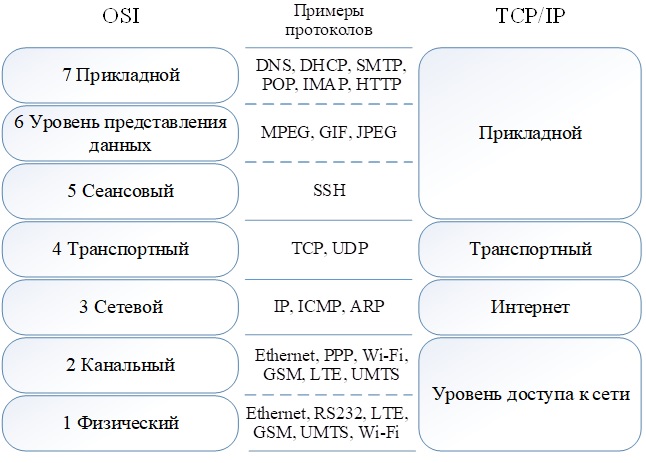


Рисунок 13 - Сравнение протоколов стека TCP/IP и модели OSI. Примеры протоколов

Следующий уровень – это Интернет или уровень межсетевого взаимодействия, на котором организуется передачей пакетов с использованием различных транспортных сетевых технологий. Этот уровень соответствует сетевому уровню модели OSI. Основной протокол Интернет-уровня – протокол IP, который отвечает за прием и передачу сегментов данных с транспортного уровня, упаковывает сообщения в пакеты и адресует пакеты для доставки конечному получателю.

Кроме того, к уровню межсетевого (Интернет) взаимодействия относятся и протоколы, регламентирующие маршрутизацию, например, протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol), который обеспечивает обратную связь от узла назначения к исходному узлу, чтобы сообщать об ошибках при доставке пакетов, а также протокол ARP, необходимый для определения MAC-адреса по известному IP-адресу.

Более высокий уровень – транспортный. Этот уровень отвечает за установление временного сеанса связи и передачу данных между двумя приложениями. Транспортный уровень — это канал между уровнем приложений и нижними уровнями, которые отвечают за передачу данных по сети. Два важнейших протокола этого уровня – это протокол управления передачей TCP (Transmission Control Protocol), обеспечивающий надежность доставки данных, и протокол дейтаграмм пользователя UDP (User Datagram Protocol), позволяющий процессу, запущенному на одном узле, отправлять пакеты процессу, запущенному на другом узле, но не подтверждающий успешную передачу датаграммы.

Верхний уровень называется прикладным или уровнем приложений. Протоколы уровня приложений используются для обмена данными между программами, выполняемыми на ЭВМ отправителя и ЭВМ получателя. Три верхних уровня модели OSI (приложений, представления и сеансовый) выполняют функции одного уровня приложений в модели TCP/IP.

Существует множество протоколов уровня приложений. Примеры наиболее известных протоколов уровня приложений:

·                   HTTP – протокол передачи гипертекста, задающий правила обмена текстами, графическими изображениями, звуковыми, видео и другими файлами мультимедиа в Интернете;

·                   FTP – протокол передачи файлов, устанавливающий правила, которые позволяют пользователю получать доступ с одной ЭВМ на другую и обмениваться файлами по сети с подтверждением и установлением соединения;

·                   IMAP – протокол доступа к сообщениям в Интернете, который позволяет клиентам получать доступ к электронным сообщениям, хранящимся на почтовом сервере, и сохраняет электронные сообщения на почтовом сервере;

·                   DNS – протокол системы доменных имен, который преобразует имена доменов в IP-адреса;

·                   SMTP – протокол электронной почты, который позволяет клиентам отправлять электронные сообщения на почтовый сервер, а также позволяет серверам отправлять электронные сообщения на другие серверы;

·                   POP – протокол электронной почты, который позволяет клиентам получать электронные сообщения с почтового сервера, а также загружать электронные сообщения с почтового сервера на компьютер;

·                   DHCP – протокол, динамически присваивающий IP-адреса клиентским ЭВМ при запуске, позволяющий также повторно использовать ненужные адреса.

**Модель взаимодействия открытых систем OSI**

Модель OSI – это базовая эталонная модель, которая обеспечивает единообразное применение производителями оборудования всех сетевых протоколов и сервисов (рисунок 1). Функции, реализуемые на каждом из уровней:

·                   *Физический уровень* – протоколы физического уровня описывают электрические, механические, функциональные и процедурные средства для установления, поддержки и разрыва физического соединения, требуемого для передачи битов из одного сетевого устройства в другое;

·                   *Канальный уровень* – описывает способы обмена кадрами данных при обмене информацией между сетевыми устройствами по общей среде передачи данных. Канальный уровень обычно делится на два по

·                   *Сетевой уровень* – позволяет реализовать обмен отдельными частями данных по сети между указанными оконечными устройствами;

·                   *Транспортный уровень* – отвечает за сегментацию, передачу и конкатенацию данных для отдельных сетевых взаимодействий между оконечными устройствами;

·                   *Сеансовый уровень* – организует обмен данными для установления связи, поддержания ее в активном состоянии и для перезапуска прерванных сеансов;

·                   *Уровень представления данных* – обеспечивает общее представление данных, передаваемых между службами прикладного уровня, отвечает за форматирование данных от исходного устройства в форму, подходящую для получения устройством назначения. Кроме того, выполняет сжатие данных, шифрование данных для передачи и дешифрование при получении;

·                   *Уровень приложений* – содержит протоколы для обмена данными между процессами.

**PDU. Принципы передачи данных по сети**

Между сетевыми устройствами могут передаваться данные самых разных видов: видео, голос, тексты, изображения. Как правило, для адаптации к пропускной способности канала, требуется разделять данные на более мелкие сегменты. Сегментация данных позволяет повысить надежность сетевого взаимодействия. При неуспешной передаче сегмента до узла назначения, повторно будет переданы только недостающие части целого сообщения.

По мере того как данные, генерируемые приложениями, передаются по стеку, различные протоколы, участвующие в обработке данных, добавляют в них информацию соответствующему каждому из уровней. Это называется инкапсуляцией.

PDU или единицей данных протокола называется та форма, которую принимают данные на каждом из уровней. В процессе инкапсуляции каждый нижестоящий уровень инкапсулирует PDU, полученную от более высокого уровня, в соответствии с используемым протоколом. На рисунке 2 показан процесс инкапсуляции данных электронной почты (рисунок 14).

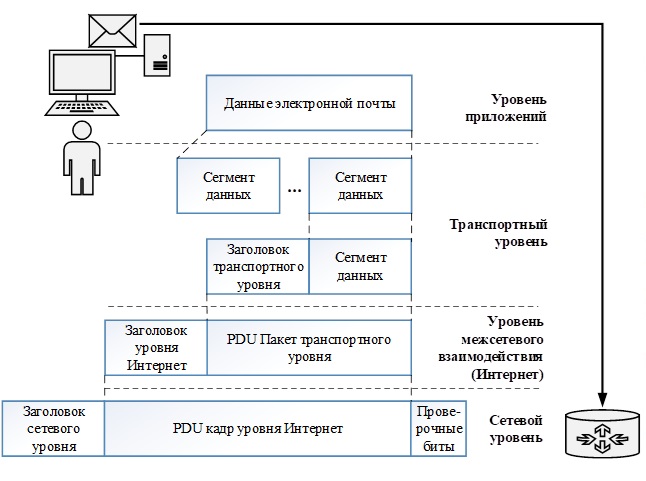


Рисунок 14 - Процесс инкапсуляции данных электронной почты в контексте стека протоколов TCP/IP.

При отправке сообщения по данные на каждом уровне оказываются вложенными внутрь инкапсулированного протокола. Например, сегмент TCP является частью данных внутри IP-пакета.

**Адреса сетевого и канального уровня**

Сетевой и канальный уровни модели OSI отвечают за передачу данных между узлом-отправителем и узлом-получателем. Адреса отправителя (Source) и получателя (Destination) сетевого уровня нужны для доставки IP-пакета от источника к месту назначения в той же или в удаленной сети.

Адреса отправителя (Source) и получателя (Destination) канального уровня требуются для передачи кадра данных от одной сетевой интерфейсной платы (NIC) к другой в той же сети.

Если отправитель и получатель IP-пакета находятся в разных сетях, кадр канала данных Ethernet не может быть отправлен напрямую к узлу получателя. Сначала кадр направляется на маршрутизатор или Default Gateway (шлюз по умолчанию). Для каждого узла в локальной сети важно правильно настроить IP-адрес основного шлюза. Все пакеты, предназначенные для отправки в удаленную сеть, направляются на Default Gateway.

# ТЕМА 3. Физические среды передачи данных. Виды подключений

## Лекция 3.1 Медный кабель: STP, UTP, коаксиальный кабель

**1.          Физические среды передачи данных. Виды подключений.**

Для передачи данных используются три вида физической среды:

·                   Медная среда: используемые сигналы являются последовательностью электрических импульсов.

·                   Оптоволоконная среда: используемые сигналы являются световым излучением.

·                   Беспроводная среда: для передачи данных используются радиосигналы микроволнового диапазона.

**1.1.   Медный кабель**

Передача данных по медным кабелям осуществляется с помощью электрических импульсов. К достоинствам медной среды можно отнести низкую стоимость кабеля и невысокое электрическое сопротивление, а к недостаткам – значительные искажения данных (затухания) при передаче на большие расстояния.

Временные и электрические характеристики импульсов, передаваемых по медной среде подвержены влиянию таких помех как:

·                   Радиочастотные и электромагнитные помехи (РЧП и ЭМП). Возможными причинами РЧП и ЭМП являются РЧ-излучение и электромагнитные устройства (например, электростанции, флуоресцентные лампы и пр.).

·                   Взаимные наводки (перекрестные помехи или межкабельные наводки) – это нежелательные электромагнитные сигналы от смежных кабелей.

Для защиты от пагубного воздействия РЧП и ЭМП некоторые виды медных кабелей оборачивают металлической экранирующей пленкой и обеспечивают требуемое заземление. Кроме того, для подавления взаимных наводок используют медные кабели, где провода каждой пары скручиваются между собой. Обеспечить защиту медного кабеля от РЧП и ЭМП можно также грамотно проектируя кабельную инфраструктуру помещения, избегая при прокладке потенциальных источников помех, и соблюдая правила прокладки и подключения медных кабелей при монтаже.

**1.1.1.     Неэкранированная витая пара (UTP)**

В настоящее время медные кабели типа неэкранированной витой пары (UTP) являются одной из самых распространенных сред передачи данных. Такие кабели с разъемами RJ-45 применяются для соединения ЭВМ с такими сетевыми устройствами, как коммутаторы (switch) и маршрутизаторы (router).

На рисунке 15 а показана структура UTP-кабеля, который состоит из четырех навитых друг на друга пар медных проводников с цветовой маркировкой, заключенных в одну гибкую пластиковую наружную оболочку, защищающую кабель от несерьезных физических повреждений.

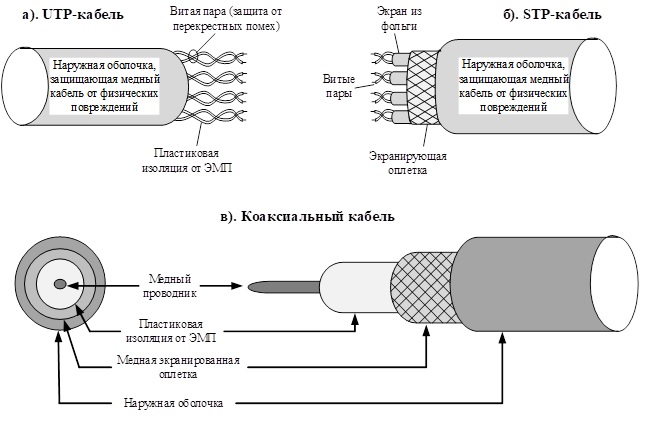


Рисунок 15 - Типы медного кабеля: а) UTP; б) STP; в) коаксиальный кабель

Существует несколько вариантов подключения отдельных проводов кабеля к различным группам контактов разъема RJ-45:

·                   Прямой кабель Ethernet (straight-through): применяется для подключения ЭВМ к коммутаторам и коммутаторов к маршрутизаторам.

·                   Кроссовый кабель Ethernet (crossover): применяется для соединения однотипных устройств (например, двух ЭВМ или двух коммутаторов).

·                   Консольный кабель (rollover): как правило, каждый вендор сетевого оборудования производит собственные кабели, которые используются для подключения ЭВМ к консольным портам маршрутизаторов или коммутаторов для выполнения их базовой конфигурации.

**Экранированная витая пара (STP)**

Использование кабелей на основе экранированной витой пары (STP) позволяет обеспечить лучшую защиту от помех, чем кабели UTP, приводя одновременно к увеличению стоимости и усложнению процедуры монтажа. Для кабелей STP также используется разъем RJ-45. Помимо экранирования для защиты от РЧП и ЭМП, в STP-кабелях применяется навивка медных проводников друг на друга для защиты от взаимных наводок. Кабели STP требуют обязательного заземления.

На рисунке 1б представлен кабель STP. Четыре пары проводников, обернуты в отдельные экраны из фольги, которые дополнительно сверху обернуты экранирующей оплеткой.

**Коаксиальный кабель**

На рисунке 1в показана структура коаксиального кабеля, состоящего из медного проводника, слоя гибкой пластиковой изоляции, медной оплетки, окружающей слой изолирующего материала и выступающая в качестве второго провода в цепи и экрана для внутреннего проводника. Снаружи кабель покрыт внешней оболочкой для защиты от небольших физических повреждений. Для коаксиального кабеля применяются различные типы разъемов.

Коаксиальные кабели могут применяться:

·                   Для подключения антенн к приемо-передающим устройствам беспроводной связи (например, в антенно-фидерных трактах базовых станций).

·                   В сетях кабельного телевидения с доступом в Интернет.

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9 (12)

## Лекция 3.2 Оптическая и беспроводная среда передачи данных. Антенны

**Физические среды передачи данных. Виды подключений.**

**Оптоволоконный кабель**

С помощью оптоволоконных кабелей можно передавать данные на б*о*льшие расстояния и с б*о*льшей пропускной способностью, чем с помощью других видов сред передачи. Затухание в оптоволокне значительно ниже, чем в медном кабеле. Кроме того, оптоволоконный кабель невосприимчив к воздействию РЧП и ЭМП. Такие кабели часто применяются для организации подключений между сетевыми устройствами. Для передачи данных по оптоволокну биты кодируются световыми импульсами.

Области применения оптоволоконных кабелей:

·                   Корпоративные сети (в качестве магистральных линий и для соединений между сетевыми устройствами).

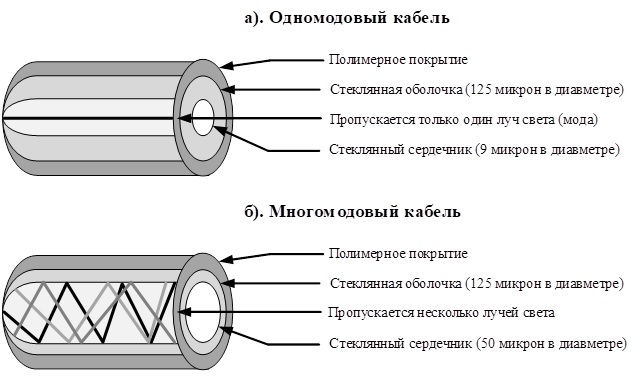
·                   «Оптоволокно до дома» (FTTH) – для организации широкополосного доступа отдельных пользователей и небольших предприятий к сети Интернет.

·                   Сети дальней связи.

·                   Подводные сети.

Оптоволоконный кабель состоит из двух стеклянных компонентов (сердечника и внутренней оболочки), а также защитной внешней оболочки. Световые импульсы, используемые для передачи данных по оптоволокну, могут генерироваться лазерами или светоизлучающими диодами (LED).

На рисунке 16 показаны оптоволоконные кабели двух типов: одномодовые и многомодовые.



*Рисунок 1*6 -Типы оптоволоконных кабелей: а) одномодовое оптоволокно; б) многомодовое оптоволокно.

Для передачи луча света по одномодовому оптоволокну (SMF) требуется дорогостоящая лазерная технология (Рис. 16 а). Такое волокно применяется для организации линий связи большой протяженности.

Многомодовое оптоволокно (MMF) имеет сердечник б*о*льшего диаметра (50-60 микрон), что позволяет передавать одновременно несколько световых лучей формируемых с помощью светодиодов (Рис.1б). Такие кабели применяют преимущественно в локальных сетях.

Волокна с сердечником многолучевого типа делятся на **шаговые и ступенчатые**. Многолучевой шаговый тип волокна так называется из-за резкой, подобно скачку, разности в показателях преломления сердечника и оболочки.

В ступенчатом сердечнике световые лучи также распространяются по волокну многолучевыми трассами, но в отличие от шагового ступенчатый сердечник содержит много слоев стекла, каждый с более низким коэффициентом преломления, в направлении от оси.

В результате такой градации световые лучи ускоряются на внешних слоях, с тем чтобы совпасть с лучами, проходящими более короткими траекториями, идущими вблизи от оси.

Волокно однолучевого типа позволяет передавать по сердечнику единичные световые лучи. Это устраняет любое искажение из-за наложения световых импульсов друг на друга. Сердечник волокна однолучевого типа мал по размеру, приблизительно 5...10 микрон

**Потери в оптоволокне**

Излучение, используемое в оптоволоконных системах, находится в инфракрасной части оптического спектра, в котором затухание при прохождении света через волокно сильно зависит от длины волны. Поэтому затухание или потери мощности должны измеряться для волн установленной длины для каждого типа волокна. Длина волны измеряется в нанометрах (нм) —— и представляет собой расстояние между двумя циклами одной и той же волны. Количество потерянной оптической энергии, вызванное поглощением и рассеиванием излучения на определенной длине волны, выражается как коэффициент затухания в децибелах на километр (дБ/км).

Потери оптической мощности на волнах разной длины происходят в волокне из-за поглощения и рассеивания.

Два диапазона длин волн — 850 и 1300 нм являются самыми распространенными и наиболее часто используемыми сегодня для передачи сигнала по стекловолоконным кабелям. Для этих длин волн промышленностью выпускаются сегодня передатчики и приемники.

***Защита оптоволокна***

Оптоволокно — очень тонкий световод. Внешние воздействия приводят к появлению микрозигзагов и, соответственно, к дополнительным потерям. Чтобы изолировать волокно от воздействия внешних сил применяют два дополнительных защитных слоя — свободный буфер и плотный буфер (рисунок 17).

*Свободный буфер* сконструирован таким образом, что волокно находится в пластиковой трубке, у которой внутренний диаметр значительно больше, чем само волокно. Как правило, внутри пластиковая трубка заполняется гелем.

Свободный буфер изолирует волокно от внешних механических повреждений, воздействующих на кабель. Многоволоконный кабель обычно состоит из нескольких таких трубок, каждая из которых содержит одно или несколько волокон, объединенных закрепляющими компонентами для защиты волокон от внешнего давления и минимизации растяжения.

*Плотный буфер* — использует прямое прессование пластика поверх основного слоя волокна. Строение плотного буфера дает возможность противостоять гораздо большей силе удара и силе давления и не влечет за собой разрыв волокна. Хотя плотный буфер более гибкий, чем свободный, оптические потери, вызванные сильными изгибами и скручиванием, из-за микроизгибов могут превышать номинальные технические нормы.

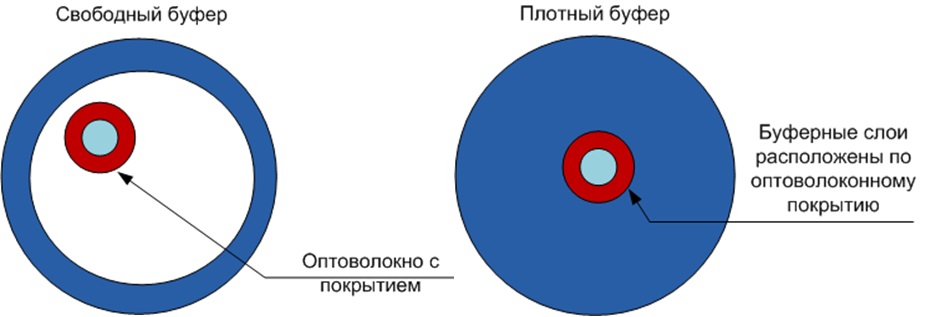


Рисунок 17 – Структура оптоволокна

*Улучшенная конструкция плотного буфера* — усиленный кабель, так называемый *кабель breakout.* В кабеле breakout волокно с плотным буфером окружено арамидной пряжей и покрытием, типа полихлорвинил. Затем одноволоконные элементы покрываются единой оболочкой для образования кабеля breakout.

**Беспроводная среда передачи данных**

В беспроводных средах данные передаются с помощью электромагнитных сигналов. Основным достоинством беспроводной среды является мобильность пользователей.

При проектировании беспроводных сетей необходимо учитывать зону покрытия и факторы ее ограничивающие, в частности возможные источники помех. Кроме того, обеспечение безопасности от несанкционированного доступа является также немаловажной задачей сетевого администратора.

Беспроводная среда – это среда, общая для всех пользователей. При одновременном подключении нескольких пользователей к локальной беспроводной сети (WLAN) или мобильной сети (PLMN), может уменьшаться пропускная способность на одного абонента, а также могут возникать коллизии. Задачи управления доступом к общей среде решаются на MAC-подуровнях соответствующими протоколами.

Подробнее познакомиться с принципами передачи данных по различным физическим средам можно в [3].

**Антенны**

**Антенны**—  устройство  для преобразования энергию высокочастотного колебания от передатчика в электромагнитную волну, способную распространяться в пространстве. Или в случае приема, производит обратное преобразование — электромагнитную волну, в ВЧ колебания (рисунок 18).  
  
**Диаграмма направленности** — графическое представление коэффициента усиления антенны, в зависимости от ориентации антенны в пространстве.

**Коэффициент усиления (КУ) антенны** — отношение мощности на входе эталонной антенны к мощности, подводимой ко входу рассматриваемой антенны. КУ является безразмерной величиной, может выражаться в децибелах (дБ, дБи, дБд). Для обозначения КУ используют латинскую букву *G* (от англ. *Gain*).

**Виды антенн:**

 -**Симметричный вибратор**

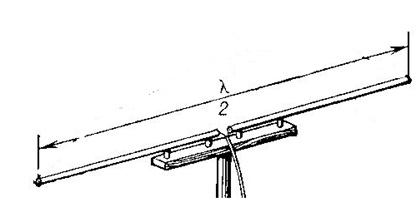


Рисунок 18 - Антенна

 В простейшем случае состоит из двух токопроводящих отрезков, каждый из которых равен 1/4 длины волны.

К примеру, если диапазон метровых волн ТВ проходит через 200 МГц, то длина волны будет равна 1,5 м.  
Каждый отрезок симметричного вибратора будет равен 0,375 метра.

**Диаграмма направленности симметричного вибратора**

В идеальных условиях, диаграмма направленности *горизонтальной плоскости (рисунок 19)*, представляет собой вытянутую восьмерку, расположенную перпендикулярно антенне. *В вертикальной плоскости*, диаграмма представляет собой окружность.

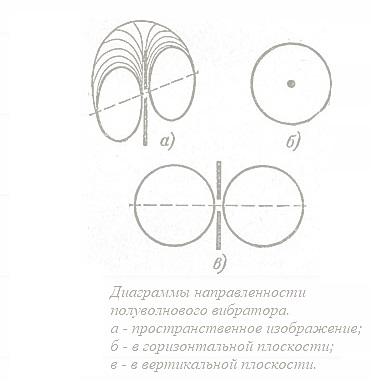


Рисунок 19- Диаграммы направленности полуволнового вибратора

В реальных условиях, на горизонтальной диаграмме присутствуют четыре небольших лепестка, расположенных под углом 90 градусов друг к другу.  
В случае не правильно подобранной длины вибратора, диаграмма направленности примет следующий вид (рисунок 20):

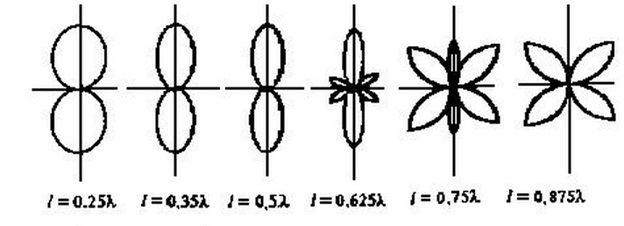


Рисунок 20 - Диаграмма направленности (выбор длины вибратора

Основное применение, в диапазонах коротких, метровых и дециметровых волн.

**Несимметричный вибратор (штыревая антенна)**

*Несимметричным*называется вибратор, у которого одно плечо по размерам или форме отличается от дру­гого (рисунок 21). *Несимметричным вертикальным заземленным виб­ратором* называется вертикальный по отношению к земле проводник, к нижнему концу ко­торого присоединен один из зажимов генератора, а другой зажим генерато­ра присоединен к земле. В качестве длины вибратора, применяют 1, 1/2 или 1/4 длины волны

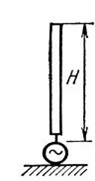


Рисунок 21 – Несимметричный вибратор

**Диаграмма направленности**

Представляет собой рассеченную вдоль «восьмерку». За счет того, что вторая половина «восьмерки» поглощается землей, коэффициент направленного действия у несимметричного вибратора в два раза больше, чем у симметричного, за счет того, что вся мощность излучается в более узком направлении (рисунок 22).  
Основное применение, в диапазонах ДВ, КВ, СВ, активно устанавливаются в качестве антенн на транспорте

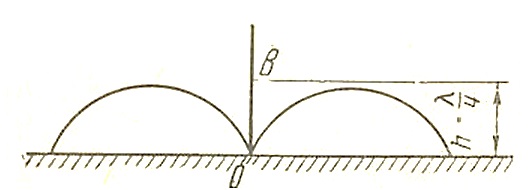


Рисунок 22 - Диаграмма направленности

**Панельные антенны**

Среди всех типов антенны наиболее распространенные - панельные антенны. Они используются как секторные антенны (рисунок 23).

Антенная решетка панельных антенн представляет собой набор диполей расположенных вертикально друг под другом. Обычно они размещаются в два столбца в левой и правой частях антенны. Тем самым реализуется пространственное горизонтальное разнесение. Этим достигается улучшение качества сигнала в направлении uplink. При этом каждый столбец диполей подключается с помощью отдельного фидера к отдельному входу оборудования БС.

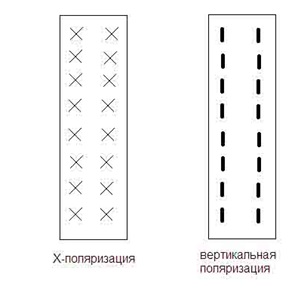


Рисунок 23 – Панельные антенны

Также могут быть установлены кросполяризованные антенны, тогда диполи будут устанавливаться Х-образно в обоих столбцах.

Для улучшения качества сигнала в направлении uplink также применяется поляризационное разнесение. При этом сигнал от мобильной станции принимается через две антенны с разной поляризацией диполей, обычно взаимно перпендикулярной. Для экономии, решетки объединяются в единый корпус что дает еще несколько вариантов антенных решеток: с вертикальной – в одной и горизонтальной – в другой поляризацией, а также с наклонами +45 и -45 градусов.



Рисунок 24 – Диаграмма панельных антенн

В настоящее время выпускается большое число различных типов панельных антенн. Наиболее существенные их различия заключаются в диаграмме направленности данных антенн. Раскрыв основного лепестка может различаться от 30 до 90 градусов, но в среднем 60-75 градусов. Также важным свойством является наклон антенны, который может быть механическим - изменяется за счет регулировки верхнего крепления панельной антенны и электрическим – зависит от наклона диполей (рисунок 24)

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9 (12)

# Тема 4. IP-адресация. Разбиение сетей на подсети

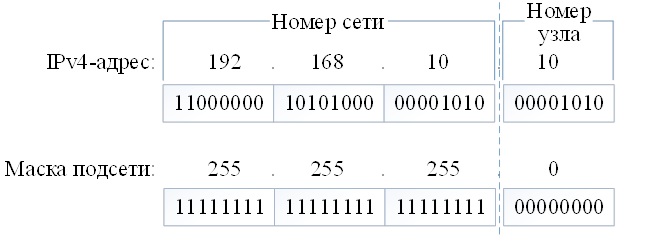
## Лекция 4.1 Адреса IPv4

**IPv4-адреса**

IP-адрес – это уникальный адрес в сети Интернет, необходимый для обеспечения межсетевого взаимодействия и осуществления обмена данными между узлами [1]. Под узлом понимается любое сетевое устройство, которое имеет возможность подключения к сети.

Каждый IP-адрес представляет собой строку из 32 бит, разделенную на 4 части, которые называются октетами. Каждый октет представляет собой 8 бит, разделенных точкой. Пример IP-адреса в двоичной системе – 11000000.10101000.00001010.00001010. Однако гораздо удобней использовать десятичную систему для обозначения IP-адресов. Так, адрес, приведенный выше, в десятичной системе исчисления будет иметь вид: 192.168.10.10.

IPv4-адрес – это иерархический адрес, состоящий из двух частей: номера сети и номера узла. На рисунке 1 показано, как одна часть битов из 32 определяет сеть, а другая — узел.



*Рисунок 25 -* Структура адреса протокола IPv4

Биты в части номера сети одинаковы для устройств, находящихся в одной сети. Биты в части узла сети уникальны для каждого узла в сети. Для того чтобы узлы могли идентифицировать, какие из 32 бит определяют сеть, а какие — узел используется маска подсети, которая побитово сравнивается с IP-адресом, выполняя логическую операцию «И» (рисунок 25).

Так как десятичное представление маски подсети для определения адресов сети узлов в виде достаточно громоздко, то часто используют другой способ обозначения маски подсети – длину префикса. Длина префикса – это количество бит, имеющих значение «1» в маске подсети. Она обозначается наклонной чертой вправо («/»).

Пример показан в таблице 1. В первом столбце перечислены различные маски подсети, которые могут использоваться с адресом узла. Во втором столбце указан 32-битный двоичный адрес. В последнем столбце указана соответствующая длина префикса.

*Таблица 1 -* Маска подсети и длина префикса

|  |  |  |
| --- | --- | --- |
| Маска подсети | 32-битный адрес | Длина префикса |
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | /8 |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | /16 |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

Сетевые адреса в одной сети делятся на адреса узлов и широковещательный адрес. Широковещательный адрес – это специальный адрес, используемый для одновременной отправки сообщения всем узлам сети, в узловой части которого одни единицы.

Устройствам в сети могут назначаться как статические (например, принтерам, серверам и сетевым устройствам), так и динамические IP-адреса. Назначение устройствам статических адресов приемлемо лишь в небольших сетях, в крупных же сетях используется динамическая IP-адресация, подразумевающая наличие DHCP-сервера, контролирующего выделение адресов узлам.

Сетевой узел (например, пользовательский терминал) — это DHCP-клиент, который запрашивает IP-адрес у DHCP-сервера. DHCP-сервер выделяет IP-адрес, маску подсети, шлюз по умолчанию и прочие параметры конфигурации. DHCP — это один из наиболее распространенных способов присвоения IPv4-адресов сетевым ЭВМ в крупных сетях. Важно, что адреса присваиваются узлам временно, на определенный период. При покидании пользователем сети, его адрес может быть повторно использован, что особенно актуально для мобильных терминалов.

**Виды адресов IPv4**

IPv4-адреса могут быть *частными* (используются в локальных сетях) и *публичными*, маршрутизируемые между сетевыми устройствами Интернет-провайдеров ISP (Internet Service Provider) на глобальном уровне.

Частными адресами являются:

·        10.0.0.0 /8 или от 10.0.0.0 до 10.255.255.255

·        172.16.0.0 /12 или от 172.16.0.0 до 172.31.255.255

·        192.168.0.0 /16 или от 192.168.0.0 до 192.168.255.255

Частные адреса нельзя использовать для доступа во внешнюю сеть Интернете, поэтому они отфильтровываются Интернет-маршрутизаторами.  Частные адреса определены в спецификациях RFC 1918.

Преобразование сетевых адресов NAT (Network Address Translation) используется для представления частного IPv4-адреса публичным. Как правило, это выполняется на маршрутизаторе, который обеспечивает соединение между внутренней сетью и сетью ISP (Default Gateway).

Существуют также специальные адреса, которые можно назначать сетевым узлам, но с ограничениями способов взаимодействия этих узлов в сети.

·     Адреса *loopback* (127.0.0.0 /8 или от 127.0.0.1 до 127.255.255.254): — это адреса, которые используют узлы, для передачи трафика самим себе, например, для проверки работоспособности конфигурации TCP/IP.

· Локальные адреса канала *Link-Local* (169.254.0.0/16 или от 169.254.0.1 до 169.254.255.254), выделяемые посредством автоматического назначения частных IP-адресов APIPA (Automatic Private IP Addressing). Они применяются в небольших одноранговых сетях или клиентами Windows DCHP для самостоятельной конфигурации в случае, если нет доступных DHCP-серверов.

·     Адреса *TEST-NET* (192.0.2.0/24 или от 192.0.2.0 до 192.0.2.255) применяются в целях обучения в качестве примера для документирования при создании сетей.

В блоке адресов от 240.0.0.0 до 255.255.255.254 имеются экспериментальные адреса, которые в соответствии с документом RFC 3330, зарезервированы для будущих нужд.

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9

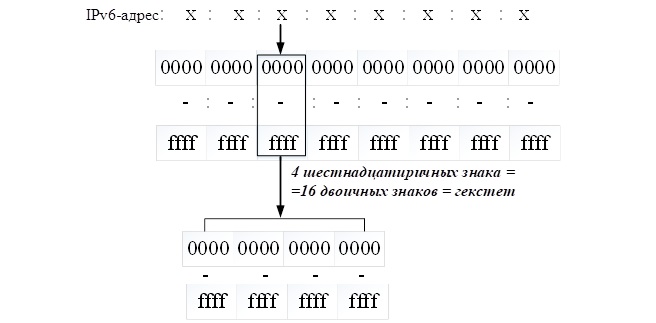
## Лекция 4.2 Адреса IPv6

**Использование адресов IPv6**

Разработкой протокола IPv6 (преемник IPv4) занималась организация IETF прежде всего для расширения адресного пространства. Помимо этого, был доработан протокол управляющих сообщений версии 6 (ICMPv6), который включает в себя разрешение и автонастройку адресов.

Максимально возможное число IPv4-адресов — 4,3 миллиарда (232). Частные адреса вместе с NAT-функцией позволили замедлить процесс истощения адресного пространства IPv4, однако потребность в его увеличении очевидна.

Длина IPv6-адреса – 128 бит, представленных в виде строки из 32 шестнадцатеричных символов. На рисунке 26 показан формат записи IPv6-адреса: x:x:x:x:x:x:x:x, где каждый «x» состоит из четырех шестнадцатеричных цифр. В IPv6-адресах 16 бит или четыре шестнадцатеричных символа часто называют гекстетом.



*Рисунок 26 -* Структура адреса протокола IPv6

Переход с IPv4 на IPv6 будет происходить постепенно, но в ближайшее время эти протоколы будут сосуществовать. IETF предлагает следующие методы для перехода сетей на протокол IPv6:

·                   Двойной стек. Этот метод позволяет протоколам IPv4 и IPv6 сосуществовать в одном и том же сегменте сети.

·                   Туннелирование. Это способ передачи пакета IPv6 через IPv4-сеть посредством инкапсуляции внутри IPv4-пакета.

·                   Преобразование сетевых адресов 64 (NAT64). IPv6-пакет преобразовывается в пакет IPv4-пакет NAT64-маршрутизатором и наоборот.

**Виды адресов IPv6**

Существует три *вида IPv6-адресов*:

·       *Индивидуальный* (или адрес одноадресной рассылки, unicast), который требуется для однозначной идентификации интерфейса на устройстве под управлением IPv6.

·       *Групповой* (или адрес многоадресной рассылки, multicast), который используется для передачи одного IPv6-пакета на несколько адресов назначения.

·       *Произвольный* (или адрес произвольной рассылки, anycast) – это любой индивидуальный IPv6-адрес, который может быть выделен нескольким сетевым устройствам. Пакет, отправляемый на адрес произвольной рассылки, передается ближайшему устройству с этим адресом.

В IPv6 нет широковещательных адресов, но существует групповой адрес, выполняющий аналогичные функции.

*Типы индивидуальных IPv6-адресов*:

·              *Глобальный индивидуальный адрес GUA* (Global Unicast Addresses) – это аналог публичного IPv4-адреса.

·              *Локальные адреса канала* (Link-local) используются для обмена данными с другими устройствами по одному локальному каналу или, что одно и то же, одной подсети.

·              У*никальный локальный индивидуальный адрес*(Unique local) используется для локальной адресации в пределах организации или между ограниченным числом организаций. Уникальные локальные адреса – это адреса в диапазоне от FC00::/7 до FDFF::7.

## Лекция 4.3 Статическая и динамическая адресация. Маска подсети IPv4. NAT

**Статическая адресация. Разделение сети IPv4 на подсети**

***Задачи IP-адресов***

Для обмена данными в Интернете узлу необходим IP-адрес. Это логический сетевой адрес конкретного узла. Для обмена данными с другими устройствами, подключенными к Интернету, необходим правильно настроенный, уникальный IP-адрес.

IP-адрес присваивается сетевому интерфейсу узла. Обычно это сетевая интерфейсная плата (NIC), установленная в устройстве. Примерами пользовательских устройств с сетевыми интерфейсами могут служить рабочие станции, серверы, сетевые принтеры и IP-телефоны. Иногда в серверах устанавливают несколько NIC, у каждой из которых есть свой IP-адрес. У интерфейсов маршрутизатора, обеспечивающего связь с сетью IP, также есть IP-адрес.

В каждом отправленном по сети пакете есть IP-адрес источника и адресата. Эта информация необходима сетевым устройствам для передачи информации адресату и передачи источнику ответа.

##### Части IP-адреса

Логический 32-битный IP-адрес представляет собой иерархическую систему и состоит из двух частей. Первая идентифицирует сеть, вторая - узел в сети. Обе части являются обязательными.

Например, если IP-адрес узла - 192.168.18.57, то первые три октета, (192.168.18), представляют собой сетевую часть адреса, а последний октет, (57) является идентификатором узла. Такая система называется иерархической адресацией, поскольку сетевая часть идентифицирует сеть, в которой находятся все уникальные адреса узлов. Маршрутизаторам нужно знать только путь к каждой сети, а не расположение отдельных узлов.

Другой пример иерархической сети - это телефонная сеть. В телефонном номере код страны, региона и станции составляют адрес сети, а оставшиеся цифры - локальный номер телефона.

При IP-адресации в одной физической сети могут существовать несколько логических сетей, если сетевая часть адреса их узла отличается. Пример. Три узла в одной физической локальной сети имеют одинаковую сетевую часть в своем IP-адресе (192.168.50), а три других узла - другую сетевую часть (192.168.70). Три узла с одной сетевой частью в своих IP-адресах имеют возможность обмениваться данными друг с другом, но не могут обмениваться информацией с другими узлами без использования маршрутизации. В данном случае имеем одну физическую сеть и две логические IP-сети.

При построении крупной сети (домена), узлы могут генерировать избыточную рассылку широковещательных запросов и негативно влиять на производительность сети: работа сети замедляется из-за значительного объема трафика, сетевые устройства также работают медленнее, так как требуется подтверждать и обрабатывать каждый пакет широковещательной рассылки.

Возможным решением данной проблемы является уменьшение размера сети путем создания меньших широковещательных доменов. Это называется разделением сети на подсети.

При разбиении сети на подсети широковещательная рассылка происходит только внутри отдельных широковещательных доменов меньшего размера.

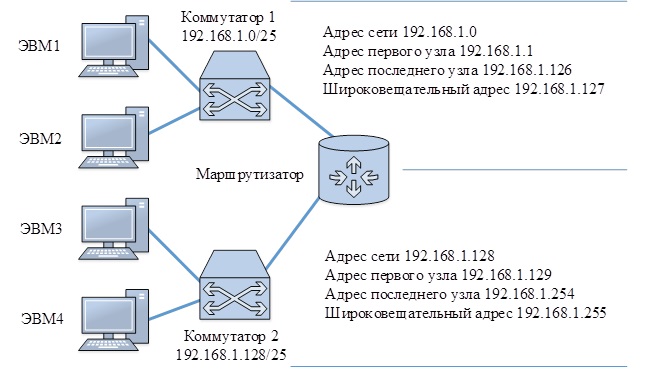
Для создания IPv4-подсетей требуется задействовать один или несколько бит из части, идентифицирующей узел, и перераспределить их в пользу бит, определяющих сеть. Для этого необходимо расширить маску подсети.

Разделение сетей удобней всего реализовать на границах октетов /8, /16 и /24. В таблице 2 определена длина этих префиксов, соответствующие маски подсети, биты сетевой (с) и узловой частей (у), а также число узлов, которые можно подключить к такой подсети.

*Таблица 2 -* Разбиение сети на подсети на границах октетов

|  |  |  |  |
| --- | --- | --- | --- |
| Длина префикса | Маска подсети | 32-битный адрес | Число узлов |
| /8 | 255.0.0.0 | уууууууу. сссссссс. сссссссс. сссссссс  11111111.00000000.00000000.00000000 | 16 777 214 |
| /16 | 255.255.0.0 | уууууууу. уууууууу.сссссссс. сссссссс  11111111.11111111.00000000.00000000 | 65 534 |
| /24 | 255.255.255.0 | уууууууу.уууууууу.уууууууу. сссссссс  11111111.11111111.11111111.00000000 | 254 |

Рассмотрим пример создания двух подсетей с помощью префикса /25. На рисунке 27 показана топология такой сети: к маршрутизатору подключены два сегмента локальной сети, каждый из которых требуется включить в подсеть.



*Рисунок 27 -* Разделение сети на две подсети /25

Для определения количества подсетей, создаваемых путем заимствования бит из узловой части адреса (*n* – число заимствованных бит), используют формулу (1):

*Число подсетей=2n.*  (1)

Максимально возможная длина префикса при разбиении на подсети равна /30 или /255.255.255.252, так как если занять последние два бита, то не останется бит для адресации узлов. Формула для определения числа узлов в подсети (2):

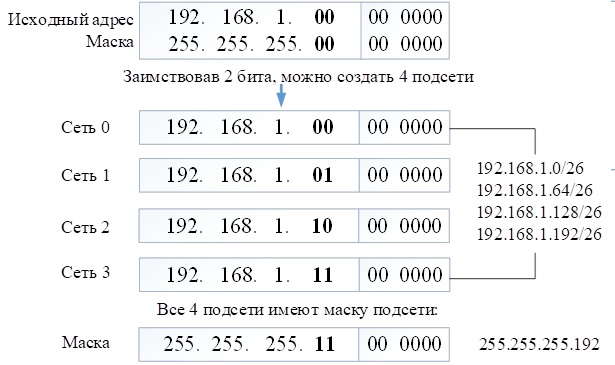
*Число узлов в подсети=2n-2.*  (2)

Два адреса в любой подсети — адрес сети и адрес широковещательной рассылки — назначить узлу нельзя, поэтому в выражении (2) вычитается 2.

На примере, показанном на рисунке 13, из узловой части адреса забирается лишь один бит, то есть остается 7 бит, поэтому число узлов в одной подсети получается следующим: 27-2 = 128-2 = 126.

Пример создания четырех подсетей с заимствованием двух бит из узловой части IP-адреса показан на рисунке 2.

Нами было рассмотрено традиционное разбиение на подсети, при котором каждой подсети выделяется одинаковое количество адресов. Однако это приводит к неэффективному использованию адресного пространства.



*Рисунок 2*8 - Пример разделения сети на четыре подсети /26

Разбиение сети на несколько подсетей с использованием маски подсети произвольной длины VLSM (Variable Length Subnet Mask) позволяет уменьшить число «лишних», неиспользованных адресов. Однако, в рамках данного курса этот способ формирования подсетей не рассматривается (рисунок 28).

##### Классы IP-адресов и маски подсети по умолчанию

IP-адрес и маска подсети совместно определяют то, какая часть IP-адреса является сетевой, а какая соответствует адресу узла (рисунок 29).

IP-адреса делятся на 5 классов. К классам A, B и C относятся коммерческие адреса, присваиваемые узлам. Класс D зарезервирован для многоадресных рассылок, а класс E - для экспериментов.

В адресах класса C сетевая часть состоит из трех октетов, а адрес узла - из одного. Выбранная по умолчанию маска подсети состоит из 24 битов (255.255.255.0). Адреса класса C обычно присваиваются небольшим сетям.

В адресах класса B сетевая часть и адрес узла состоят из двух октетов. Выбранная по умолчанию маска подсети состоит из 16 бит (255.255.0.0). Обычно эти адреса используются в средних сетях.

В адресах класса A сетевая часть состоит всего их одного октета, остальные отведены узлам. Выбранная по умолчанию маска подсети состоит из 8 бит (255.0.0.0). Обычно такие адреса присваиваются крупным организациям.

Класс адреса можно определить по значению первого октета. Например, если значение первого октета IP-адреса находится в диапазоне от 192 до 223, то это адрес класса C., например, адрес 200.14.193.67 относится к классу С.

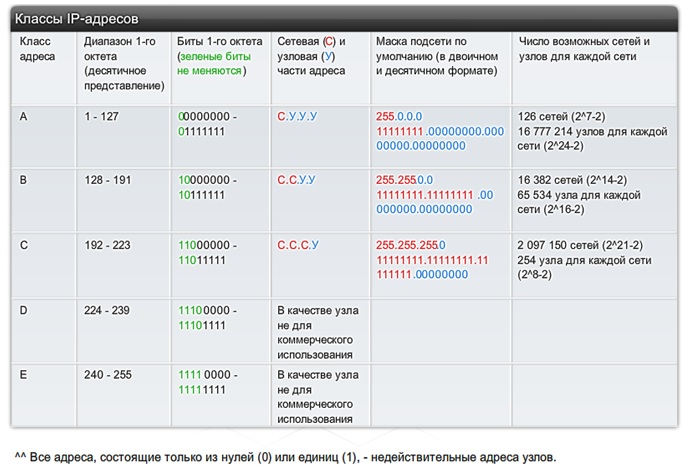


Рисунок 29 – Классы IP-адресов

##### Общие и частные IP-адреса

Всем узлам, подключенным непосредственно к Интернету, необходим уникальный глобальный (публичный) IP-адрес. Поскольку количество 32-битных адресов конечно, существует риск, что их не хватит. В качестве одного из решений было предложено зарезервировать некоторое количество частных адресов для использования только внутри организации. Таким образом, внутренние узлы смогут обмениваться данными друг с другом без уникальных общих IP-адресов.

В соответствии со стандартом RFC 1918 несколько диапазонов адресов класса A, B и C были зарезервированы. Как видно на рисунке 30, в диапазон частных адресов входит одна сеть класса A, 16 сетей класса B и 256 сетей класса C. Таким образом, сетевые администраторы получили определенную степень свободы в плане предоставления внутренних адресов.

В очень большой сети можно использовать частную сеть класса A, где можно создать более 16 миллионов частных адресов.

В средних сетях можно использовать частную сеть класса B с более чем 65 000 адресов.

В домашних и небольших коммерческих сетях обычно используется один частный адрес класса C, рассчитанный на 254 узла.

Одну сеть класса A, 16 сетей класса B или 256 сетей класса C могут использовать организации любого размера. Многие организации пользуются частной сетью класса A.



Рисунок 30 – Резервирование сетевых адресов

Узлы из внутренней сети организации могут использовать частные адреса до тех пор, пока им не понадобится прямой выход в Интернет. Соответственно, один и тот же набор адресов подходит для нескольких организаций. Частные адреса не маршрутизируются в Интернете и быстро блокируются маршрутизатором Интернет-провайдера.

Частные адреса можно использовать как меру безопасности, поскольку они видны только в локальной сети, а посторонние получить прямой доступ к этим адресам не могут.

Кроме того, существуют частные адреса для диагностики устройств. Они называются адресами обратной связи. Для таких адресов зарезервирована сеть 127.0.0.0 класса А.

##### Адреса одноадресных, широковещательных и многоадресных рассылок

Помимо классов, IP-адреса делятся на категории, предназначенные для одноадресных, широковещательных или многоадресных рассылок. С помощью IP-адресов узлы могут обмениваться данными в режиме "один к одному" (одноадресная пересылка), "один ко многим"; (многоадресная рассылка) или "один ко всем" (широковещательная рассылка).

##### Одноадресная рассылка

Адрес одноадресной рассылки чаще всего встречается в сети IP. Пакет с одноадресным получателем предназначен конкретному узлу. Пример: узел с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера с IP-адресом 192.168.1.200 (адресат).

Для отправки и приема одноадресного пакета IP-адрес получателя должен находиться в заголовке IP-пакета. Кроме того, в заголовке кадра Ethernet должен быть MAC-адрес получателя. IP-адрес и MAC-адрес - это данные для доставки пакета одному узлу.

##### Широковещательная рассылка

В пакете широковещательной рассылки содержится IP-адрес получателя, где в отведенной узлу части есть только единицы (1). Это означает, что пакет получат и обработают все узлы в локальной сети (домене широковещательной рассылки). Широковещательные рассылки предусмотрены во многих Интернет-протоколах, например, ARP и DHCP.

В сети класса C 192.168.1.0 с маской подсети по умолчанию 255.255.255.0 используется адрес широковещательной рассылки 192.168.1.255. В отведенной узлу части стоит 255, или двоичное 11111111 (все единицы).

В сети класса B 172.16.0.0 с маской подсети по умолчанию 255.255.0.0 используется адрес широковещательной рассылки 172.16.255.255.

В сети класса A 10.0.0.0 с маской подсети по умолчанию 255.0.0.0 используется адрес широковещательной рассылки 10.255.255.255..

Для сетевого IP-адреса широковещательной рассылки нужен соответствующий MAC-адрес в кадре Ethernet. В сетях Ethernet используется широковещательный MAC-адрес из 48 единиц, который в шестнадцатеричном формате выглядит как FF-FF-FF-FF-FF-FF.

##### Многоадресная рассылка

Адреса многоадресных рассылок позволяют источнику рассылать пакет группе устройств.

Устройства, принадлежащие к многоадресной группе, получают ее IP-адрес. Диапазон таких адресов - от 224.0.0.0 до 239.255.255.255. Поскольку адреса многоадресных рассылок соответствуют группам адресов (которые иногда называются группами узлов), они используются только как адресаты пакета. У отправителя всегда одноадресный адрес.

Адреса многоадресных рассылок используются, например, в дистанционных играх в которых участвует несколько человек из разных мест. Другой пример - это дистанционное обучение в режиме видеоконференции, где несколько учащихся подключаются к одному и тому же курсу.

Как и одноадресным и широковещательным адресам, IP-адресам многоадресной рассылки нужен соответствующий MAC-адрес, позволяющий доставлять кадры в локальной сети. Многоадресный MAC-адрес - это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E. Нижние 23 бита IP-адреса многоадресной группы преобразуются в остальные 6 шестнадцатеричных символов адреса Ethernet. Пример (см. рисунок) - шестнадцатеричное значение 01-00-5E-0F-64-C5. Каждому шестнадцатеричному символу соответствует 4 двоичных бита.

**Динамические адреса**

Список пользователей локальной сети часто меняется. Появляются новые пользователи с ноутбуками, которые нужно подключить. Другие устанавливают новые рабочие станции. Чтобы каждой станции не приходилось вручную присваивать IP-адреса, проще всего это сделать автоматически. Для этого используется протокол под названием Dynamic Host Configuration Protocol (DHCP).

DHCP предусматривает механизм автоматического присвоения информации об адресе (рисунок 31), например, IP-адреса, маски подсети, шлюза по умолчанию и других настроек.

Это наиболее предпочтительный способ присвоения IP-адресов узлам в большой сети, поскольку он облегчает работу специалистов службы поддержки и практически устраняет возможность ошибки.

Другое преимущества DHCP состоит в том, что адреса присваиваются узлам временно. Если узел выключается или уходит из сети, его адрес возвращается в пул для повторного использования. Это особенно полезно для мобильных пользователей, которые то подключаются, то отключаются.

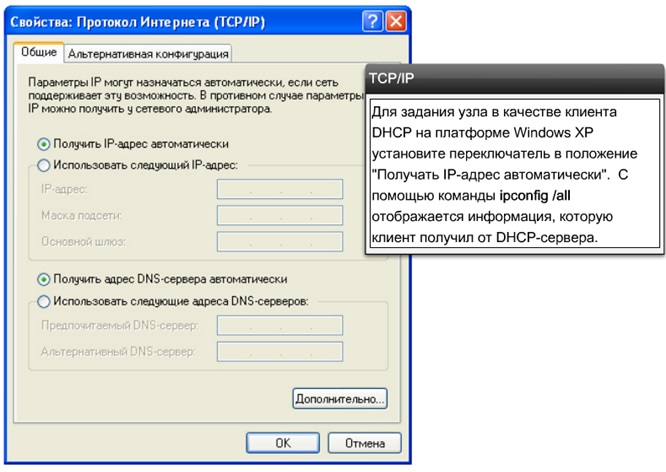


Рисунок 31 – Автоматическое получение IP-адреса

##### Серверы DHCP

Когда вы подключаетесь к беспроводной сети в аэропорту или магазине, доступ в Интернет обеспечивает DHCP. При входе в зону связи установленный на ноутбуке клиент DHCP связывается с локальным сервером DHCP через беспроводное соединение. Сервер DHCP присваивает ноутбуку IP-адрес.

В качестве серверов DHCP могут выступать самые разные устройства при условии, что на них установлено служебное ПО DHCP. В большинстве средних и крупных сетей сервер DHCP - это локальный выделенный сервер на базе ПК.

В домашних сетях он обычно находится у Интернет-провайдера. Узел из домашней сети получает настройки IP непосредственно от Интернет-провайдера.

Во многих домашних и небольших корпоративных сетях для подключения к модему Интернет-провайдера используется встроенный маршрутизатор. В данном случае он выступает в качестве клиента и сервера DHCP. В качестве клиента он получает настройки IP от Интернет-провайдера, а затем, уже как сервер DHCP, передает их внутренним узлам локальной сети.

Помимо серверов на базе ПК и встроенных маршрутизаторов, услуги DHCP могут предоставлять клиентам и другие сетевые устройства, например, выделенные маршрутизаторы. Такое встречается реже.

При первой настройке в качестве клиента DHCP у узла нет IP-адреса, маски подсети и шлюза по умолчанию. Он получает эти данные от сервера DHCP, локального или принадлежащего Интернет-провайдеру. На сервере DHCP настраивается диапазон, или пул, IP-адресов, которые можно присвоить клиентам DHCP.

Клиент, которому нужен IP-адрес, посылает сообщение о поиске DHCP в виде широковещательной рассылки с IP-адресом получателя 255.255.255.255 (32 единицы) и MAC-адресом получателя FF-FF-FF-FF-FF-FF (48 единиц). Кадр DHCP получат все узлы в сети, но ответит только сервер DHCP. Он отправляет источнику предложенный IP-адрес клиента. Узел в ответ посылает на указанный сервер запрос DHCP с подтверждением использования IP-адреса. Сервер присылает подтверждение.

В большинстве домашних и небольших корпоративных сетей услуги DHCP предоставляет локальным сетевым клиентам многофункциональное устройство. Для настройки беспроводного маршрутизатора Linksys нужно войти в веб-интерфейс: открыть обозреватель и ввести в поле "Address" IP-адрес маршрутизатора по умолчанию: 192.168.1.1. Откройте окно настройки DHCP.

IP-адрес 192.168.1.1 и маска подсети 255.255.255.0 выбраны для интерфейса встроенного маршрутизатора по умолчанию. Это шлюз по умолчанию для всех узлов в локальной сети и IP-адрес встроенного сервера DHCP. По умолчанию у большинства беспроводных маршрутизаторов и других домашних встроенных маршрутизаторов сервер DHCP включен.

В окне настройки DHCP можно выбрать диапазон DHCP по умолчанию или указать начальный адрес диапазона DHCP (не используйте 192.168.1.1) и количество присваиваемых адресов. Кроме того, можно изменить время выделения (по умолчанию 24 часа). Функция настройки DHCP у большинства Интернет-провайдеров предоставляет информацию о подключенных узлах и IP-адресах, соответствующих MAC-адресах и времени выделения

#### Преобразование сетевых адресов

Встроенный маршрутизатор получает от Интернет-провайдера общий адрес, позволяющий отправлять и получать пакеты через Интернет. Он, в свою очередь, предоставляет локальным сетевым клиентам частные адреса. Поскольку в Интернете частные адреса не используется, при входе клиентов в Интернет их нужно преобразовать в уникальные общие адреса.

Процесс преобразования частных адресов в маршрутизируемые в Интернете адреса называется преобразованием сетевых адресов (NAT). С помощью NAT частный (локальный) IP-адрес источника превращается в общий (глобальный) адрес. Входящие пакеты проходят обратный процесс. Используя NAT, встроенный маршрутизатор может преобразовать многие внутренние IP-адреса в один общий.

Преобразовывать нужно только адреса пакетов, которые идут в другие сети. Они в обязательном порядке проходят через шлюз, где встроенный маршрутизатор заменяет частный IP-адрес узла-источника своим общим IP-адресом.

Хотя каждому узлу во внутренней сети присвоен уникальный частный адрес IP, они используют один и тот же маршрутизируемый в Интернете адрес встроенного маршрутизатора.

# Тема 5. Основы телекоммуникационных сетей

## Лекция 5.1 Аналоговые и цифровые сигналы. АЦП и ЦАП. Спектр сигналов

##### АНАЛОГОВЫЙ И ЦИФРОВОЙ СИГНАЛ

Аналоговый сигнал (иначе непрерывный) - сигнал данных, у которого каждый из параметров описывается функцией времени и непрерывным множеством возможных значений (рисунок 32).

Применение: Аналоговые сигналы часто используют для представления непрерывно изменяющихся физических величин. Например, аналоговый электрический сигнал, снимаемый с термопары, несет информацию об изменении температуры, сигнал с микрофона — о быстрых изменениях давления в звуковой волне, и т. п.

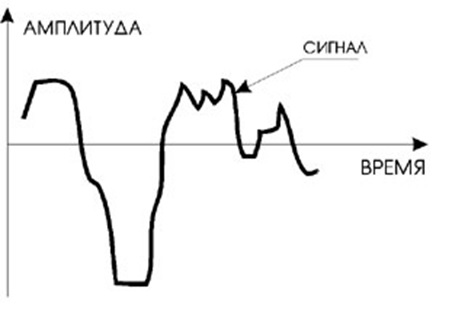


Рисунок 32 – Аналоговый сигнал АЧХ

Отсутствие чётко отличимых друг от друга дискретных уровней сигнала приводит к невозможности применить для его описания понятие информации в том виде, как она понимается в цифровых технологиях.

Аналоговые сигналы описываются некоторой математической функцией времени.

Самым распространенным сигналов в телекоммуникационных сетях является синусоидальный сигнал, записываемый как    s(t) = A·cos(ω·t + φ)

Аналоговые сигналы используются в телефонии, радиовещании, телевидении. Ввести такой сигнал в компьютер и обработать его невозможно, так как на любом интервале времени он имеет бесконечное множество значений, а для точного (без погрешности) представления его значения требуются числа бесконечной разрядности. Поэтому необходимо преобразовать аналоговый сигнал так, чтобы можно было представить его последовательностью чисел заданной разрядности.

Электрический аналоговый сигнал возникает, когда физический сигнал (например, речь) некоторым устройством преобразовывается в электрический.

Аналоговое представление сигнала наиболее точно, однако малейшее искажение формы несущего электрического сигнала неизбежно повлечет за собой такое же искажение формы и сигнала переносимого. В терминах теории информации, количество информации в несущем сигнале в точности равно количеству информации в сигнале исходном, и электрическое представление не содержит избыточности, которая могла бы защитить переносимый сигнал от искажений при хранении, передаче и усилении.

Цифровое представление электрических сигналов призвано внести в них избыточность, предохраняющую от воздействия паразитных помех. Для этого на несущий электрический сигнал накладываются серьезные ограничения - его амплитуда может принимать только два предельных значения - 0 и 1.

Для представления аналогового сигнала последовательностью чисел конечной разрядности, его преобразовывают в дискретный сигнал, а затем квантуют. Сигнал представляется таким образом, что на каждом заданном промежутке времени известно приближённое (квантованное) значение сигнала, которое можно записать целым числом. Если записать эти целые числа в двоичной системе, получится последовательность нулей и единиц, которая и будет являться цифровым сигналом.

##### Аналогово-цифровое преобразование (АЦП)

Аналоговый сигнал обрабатывается в специальном блоке: аналогово-цифровом преобразователе (АЦП).

Существуют также устройства обратного действию АЦП, это Цифро-аналоговые преобразователи (ЦАП). К примеру, они используются в ТВ-ресиверах, то есть когда телевизионное устройство не способно обработать цифровой сигнал и необходимо восстановить аналоговый сигнал из цифрового.

**Принцип действия АЦП:**

В АЦП преобразование аналогового сигнала в цифровой происходит по истечению 2х этапов: Дискретизация по времени и квантование по амплитуде.

**Дискретизация аналогового сигнала по времени**

Процесс дискретизации по времени — это процесс получения мгновенных значений преобразуемого аналогового сигнала с определенным временным шагом, называемым шагом дискретизации. Например, если частота дискретизации равна 44,1 кГц, это значит, что сигнал измеряется 44100 раз в течение секунды. Основной задачей на первом этапе преобразования аналогового сигнала в цифровой (оцифровки) является выбор частоты дискретизации аналогового процесса. Решить ее помогает **теорема Котельникова — Найквиста**, утверждающая, что для того, чтобы аналоговый (непрерывный по времени) сигнал, занимающий полосу частот от 0 до F Гц, можно было абсолютно точно восстановить по его отсчетам, частота дискретизации должна быть как минимум вдвое больше максимальной звуковой частоты Fmax.

Общий вид теоремы (рисунок 33):  **Fдискретизации ≥ 2Fmax**

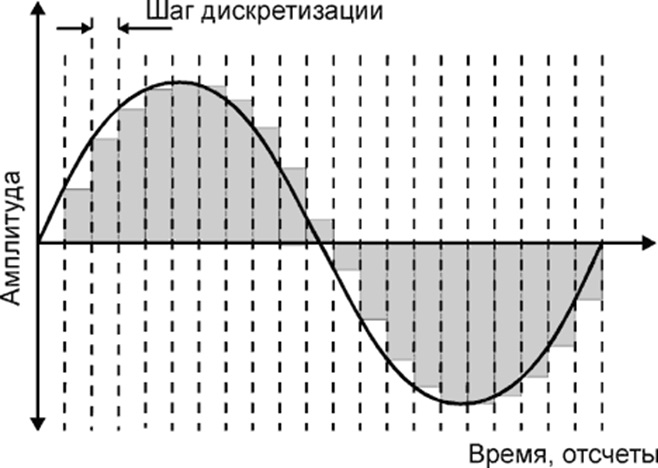


Рисунок 33 – Дискретизация

**Квантование амплитуды дискретных отсчетов**

При квантовании (рисунок 34) вся область значений сигнала разбивается на уровни, количество которых должно быть представлено в числах заданной разрядности. Расстояния между этими уровнями называется шагом квантования  Δ. Число этих уровней равно N (от 0 до N-1). Каждому уровню присваивается некоторое число. Отсчёты сигнала сравниваются с уровнями квантования и в качестве сигнала выбирается число, соответствующее некоторому уровню квантования. Каждый уровень квантования кодируется двоичным числом с n разрядами. Число уровней квантования N и число разрядов n двоичных чисел, кодирующих эти уровни, связаны соотношением n≥log2(N).

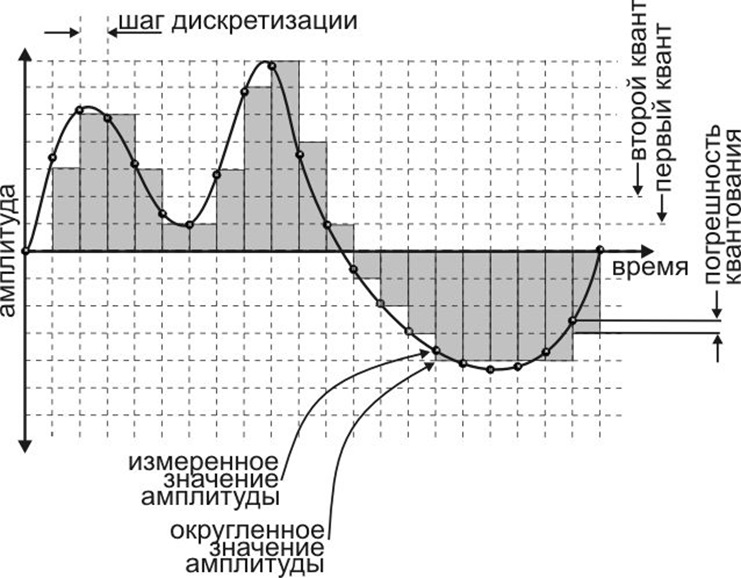


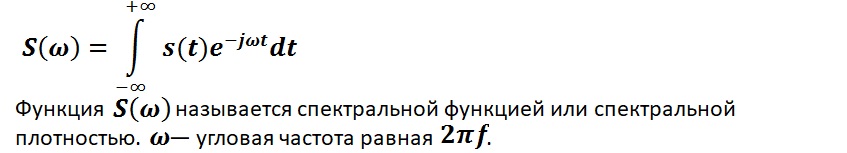
Рисунок 34 - Квантование

#### Представление сигнала

Существует два способа представления сигнала в зависимости от области определения: ***временной и частотный***. В первом случае сигнал представляется функцией времени  характеризующей изменение его параметра.

Кроме временного представления сигналов и функций при анализе и обработке данных широко используется описание сигналов функциями частоты. Действительно, любой сколь угодно сложный по своей форме сигнал можно представить в виде суммы более простых сигналов, и, в частности, в виде суммы простейших гармонических колебаний, совокупность которых называется частотным спектром сигнала.

Для перехода к частотному способу представления используется **преобразование Фурье**:



***Спектр сигнала*** — в радиотехнике это результат разложения сигнала на более простые в базисе ортогональных функций.

В радиотехнике в качестве базисных функций используют ***синусоидальные функции***. Это объясняется рядом причин:

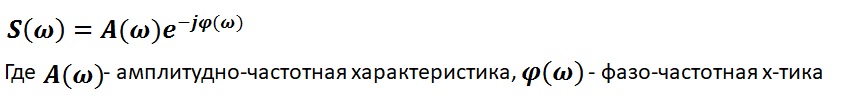
•Эти функции являются простыми и определены при всех значениях t, являются ортогональными и составляют полный набор при кратном уменьшении периода;

•гармоническое колебание является единственной функцией времени, сохраняющей свою форму при прохождении колебания через линейную систему с постоянными параметрами, могут только изменяться амплитуда и фаза;

•для гармонических функций имеется математический аппарат комплексного анализа;

•гармоническое колебание легко реализуемо на практике.

Спектр сигнала является комплексной величиной и представляется в виде:



## Лекция 5.2 Основы шифрования данных

**Шифрование**

 - это процесс преобразования открытых данных в зашифрованные. Математически это выглядит как:

**С = Ek1(M)**

**<p>M' = Dk2(C)**,

где M (message) - открытая информация ("исходные данные");

 C (cipher text) - полученный в результате зашифрования шифртекст (криптограмма);

 E (encryption) – функция шифрования, выполняющая по определенному алгоритму криптографические преобразования над исходными данными;

 k1 (key) - параметр функции E, называемый ключом шифрования;

 M' - информация, полученная в результате дешифрования;

 D (decryption) - функция дешифрования, выполняющая обратные шифрованию криптографические преобразования над шифр-текстом;

 k2 - ключ, с помощью которого выполняется дешифрование информации.

Ключ (ГОСТ 28147-89) - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований". Это случайная или специальным образом созданная по паролю последовательность бит, являющаяся переменным параметром алгоритма шифрования..

Чтобы результат дешифрования совпал с исходным сообщением (т. е. чтобы M' = M), необходимо выполнение двух условий: 1. функция дешифрования D должна соответствовать функции шифрования E. 2. ключ дешифрования k2 должен совпадать с  ключом шифрования k1.

**Алгоритмы шифрования делятся на две категории**: симметричного (AES, ГОСТ, Blowfish, CAST, DES) и асимметричного (RSA, El-Gamal) шифрования.

Для симметричных соотношение ключей шифрования и дешифрования определяется как k1 = k2 = k (т. е. функции E и D используют один и тот же ключ шифрования).

При асимметричном шифровании ключ шифрования k1 вычисляется по ключу k2 таким образом, что обратное преобразование невозможно.

**Стойкость алгоритма шифрования**

*Криптостойкость* - основная характеристика алгоритмов шифрования и указывает прежде всего на степень сложности получения исходного текста из зашифрованного без ключа k2. Алгоритм шифрования считается стойким до тех пор, пока не будет доказано обратное.

Для того чтобы взломать алгоритм шифрования нужно:

•Иметь в распоряжении криптосистему (т.е. программу) и примеры зашифрованных сообщений.

•Знать криптографический протокол - как программа шифрует данные.

•Реализовать алгоритм перебора ключей для этой криптосистемы.

*Шифрование обеспечивает дополнительный уровень безопасности конфиденциальных данных, защищая файлы на компьютере и передаваемую по сети информацию от посторонних пользователей, шпионов и всех, кому не разрешен доступ к информации конфиденциального характера. Чтобы данные с легкостью не оказались у третьих лиц, необходимо использовать шифрование, т.к. более эффективного способа их защиты пока не существует.*

##### Когда требуется шифрование?

Шифрование необходимо для работы со всеми данными, чувствительными для бизнеса. Такие данные могут обрабатываться и храниться на жестких дисках, переносных устройствах, в электронных письмах, файлах, папках и в других местах. Существует ряд специфических угроз, для своевременного предотвращения которых обязательно требуется использовать шифрование:

* **Кража компьютерного оборудования**

При краже и потере компьютерной техники данные, хранящиеся на незашифрованных дисках и других носителях информации, при попадании в руки злоумышленника могут быть без труда прочитаны и проданы заинтересованным лицам, в том числе конкурентам. Кроме того, в случае внезапных проверок и изъятия компьютерного оборудования представителями госорганов информация конфиденциального характера может стать известной посторонним.

* **Промышленный шпионаж**

Участившиеся инциденты промышленного шпионажа, наблюдаемые за последнее время, связаны с высоким уровнем финансовых рисков. Шпион, которым может быть кто угодно, даже самый «надежный» сотрудник, может получить доступ к компьютеру с хранящимися на нем критически важными данными в незашифрованном виде.

* **Компромат**

При физическом доступе к компьютеру злоумышленник может разместить на нем любую нежелательную информацию и оповестить об этом заинтересованных лиц. Последствия при этом могут быть самыми непредсказуемыми.

* **Халатность сотрудников**

Если сотрудник внезапно покинул рабочее место и забыл заблокировать компьютер, информация может стать доступной посторонним лицам и использоваться для причинения серьезного ущерба владельцу информации.

Кроме того, сотрудник может по ошибке направить информацию конфиденциального характера не доверенному адресату.

##### Основные преимущества шифрования данных

* надежная защита регулярно используемой в бизнес-деятельности компании конфиденциальной информации в электронном виде;
* защита от несанкционированного доступа баз данных, корпоративной почты и другой информации;
* предоставление доступа к конфиденциальным данным только доверенным сотрудникам;
* экстренная блокировка доступа к данным;
* защита от копирование данных нелояльным или подкупленным сотрудником, который может иметь физический доступ к компьютерному оборудованию.
* снижение рисков прямых и косвенных финансовых потерь вследствие утечки важной для бизнеса информации;
* повышение уровня доверия клиентов и партнеров;
* повышение уровня корпоративной бизнес-этики при внешнем и внутреннем информационном обмене электронными сообщениями;
* обеспечение уверенности в надежной защите конфиденциальной информации.

**Блок схема алгоритма шифрования ГОСТ 28147-8**

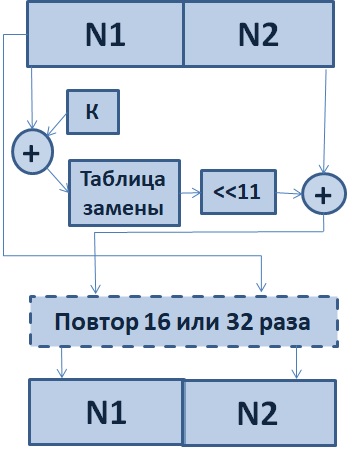


Рисунок 35 - **Блок схема алгоритма шифрования ГОСТ 28147-8**

**ГОСТ 28147-8.**Стандарт Российской Федерации на шифрование и защиту данных. В 1989 году стал официальным стандартом СССР, а позже, после распада СССР, федеральным стандартом Российской Федерации.

Размер ключа, бит - 256

Этот алгоритм (рисунок 35) шифрует информацию блоками по 64 бит, которые затем разбиваются на два субблока по 32 бит (N1 и N2). Субблок N1 обрабатывается определенным образом, после чего его значение складывается со значением субблока N2 (сложение выполняется по модулю 2, XOR - "исключающее или"), а затем субблоки меняются местами. Такое преобразование выполняется определенное число раз ("раундов"): 16 или 32 в зависимости от режима работы алгоритма. В каждом раунде выполняются две операции: 1. субблок N1 складывается по модулю 2 с 32-битами частью ключа K. 2. После наложения ключа субблок N1 разбивается на 8 частей по 4 бита, значение каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитовый циклический сдвиг субблока влево на 11 бит.

**Процедура генерации ключа шифрования в 3G/4G мобильной сети (AKA - Authentication Key Agreement)**

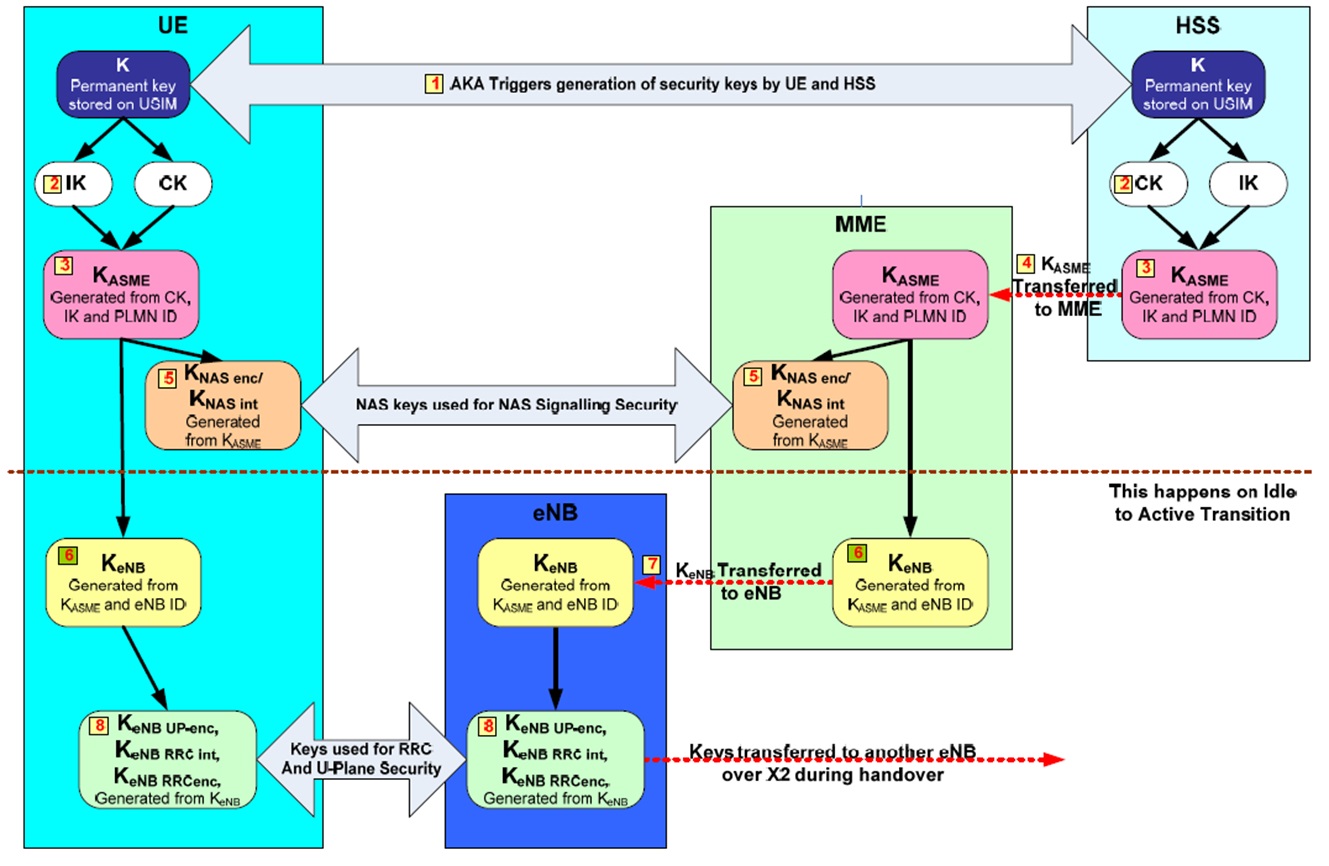


Рисунок 36 - Блок-схема генерации ключей в мобильной связи 4-го поколения LTE

На рисунке 36 показана блок-схема генерации ключей в мобильной связи 4-го поколения LTE (алгоритм AKA), где UE (User Equipment) - пользовательский терминал,  eNB - базовая станция (точка радиодоступа), MME (Mobility Management Entity) - элемент управления мобильностью, HSS (Home Subscriber Server) -  Сервер домашних абонентов, на котором хранятся ключи для шифрования (CK- Ciphering Key) и защиты целостности данных (IK- Integrity Protection Key) идентичные тем ключам, что сохранены на SIM-карте абонента, из которых зачем вычиляются промежуточные ключи и окончательные параметры для шифрования данных радиоинтерфейса (xxeNB) и сигнальных сообщений НЕ-уровня доступа (NAS -Non-Access-Stratum)

## Лекция 5.3 Помехоустойчивое кодирование данных

#### Помехоустойчивое кодирование

**Понятие корректирующего кода**

Теория помехоустойчивого кодирования базируется на результатах исследований, проведенных Клодом Шенноном. Он сформулировал теорему для дискретного канала с шумом: при любой скорости передачи двоичных символов, меньшей, чем пропускная способность канала, существует такой код, при котором вероятность ошибочного декодирования будет сколь угодно мала.

Построение такого кода достигается путем введения избыточности. Такие коды называют избыточными или корректирующими. Корректирующие свойства избыточных кодов зависят от правил построения этих кодов и параметров кода (длительности символов, числа разрядов, объема избыточности и др.).

По сути, кодирование — это добавление к исходной информации дополнительной, проверочной информации. Для кодирования на передающей стороне используются кодер, а на принимающей стороне — используют декодер для получения исходного сообщения.

Избыточность кода — это количество проверочной информации в сообщении. Рассчитывается она по формуле:

k/(i+k), где

 k — количество проверочных бит,

 i — количество информационных бит.

Например, мы передаем 3 бита и к ним добавляем 1 проверочный бит — избыточность составит 1/(3+1) = 1/4 (25%).

**Код с проверкой на четность**

 Проверка четности – простой метод для обнаружения ошибок в передаваемом пакете данных. С помощью данного кода нельзя восстановить исходные данные, но можно обнаружить одиночную ошибку.

 В каждом пакете данных есть один бит четности, или, так называемый, паритетный бит. Этот бит устанавливается во время записи (или отправки) данных, и затем рассчитывается и сравнивается во время чтения (получения) данных. Он равен сумме по модулю 2 всех бит данных в пакете. То есть число единиц в пакете всегда будет четно. Изменение этого бита (например ,с 0 на 1) сообщает о возникшей ошибке (рисунок 37).

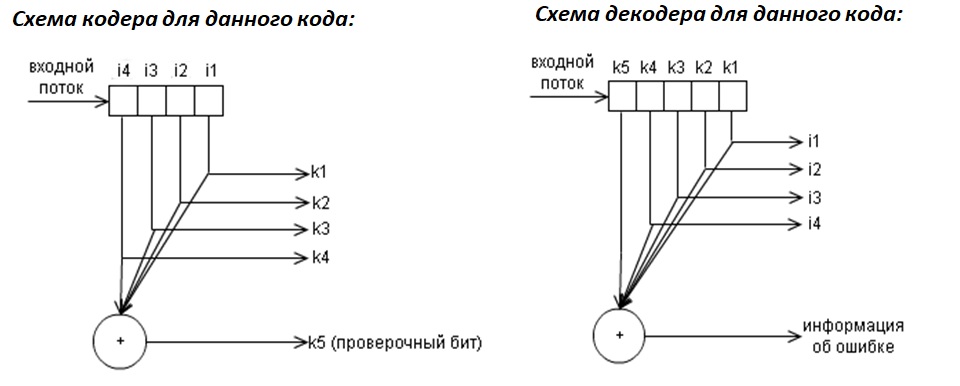


Рисунок 37 – Схемы кодера и декодера

Пример:

Начальные данные: 1111

 Данные после кодирования: 11110 ( 1 + 1 + 1 + 1 = 0 (mod 2) )

 Принятые данные: 10110 (изменился второй бит)

 Как мы видим, количество единиц в принятом пакете нечетно, следовательно, при передаче произошла ошибка.

Этот метод служит только для определения одиночной ошибки. В случае изменения состояния двух битов, возможна ситуация, когда вычисление контрольного бита совпадет с записанным. В этом случае система не определит ошибку, а это не есть хорошо.

Например:

Начальные данные: 1111

 Данные после кодирования: 11110 ( 1 + 1 + 1 + 1 = 0 (mod 2) )

 Принятые данные: 10010 (изменились 2 и 3 биты)

 В принятых данных число единиц четно, и, следовательно, декодер не обнаружит ошибку.

 Так как около 90% всех нерегулярных ошибок происходит именно с одиночным разрядом, проверки четности бывает достаточно для большинства ситуаций.

**Код Хэмминга**

Ричард Хэмминг разработал код, который обеспечивает обнаружение и исправление одиночных ошибок при минимально возможном числе дополнительных проверочных бит. Для каждого числа проверочных символов используется специальная маркировка вида (k,i)=(2i-1, 2i-1-i), где k — количество символов в сообщении, i — количество информационных символов в сообщении (рисунок 38).

Например, существуют коды (7, 4), (15, 11), (31, 26). Каждый проверочный символ в коде Хэмминга представляет сумму по модулю 2 некоторой подпоследовательности данных. Рассмотрим пример, когда количество информационных бит i в блоке равно 4 — это код (7,4), количество проверочных символов равно 3. Классически, эти символы располагаются на позициях, равных степеням двойки в порядке возрастания:

•первый проверочный бит на 20 = 1;

• второй проверочный бит на 21 = 2;

• третий проверочный бит на 22 = 4;

 но можно и разместить их в конце передаваемого блока данных (тогда формула для их расчета будет другая).  Рассчитаем эти проверочные символы:

r1 = i1 + i2 + i4

 r2 = i1 + i3 + i4

 r3 = i2 + i3 + i4

 Итак, в закодированном сообщении получится следующее:

r1 r2 i1 r3 i2 i3 i4

Минимальное кодовое расстояние является важнейшей характеристикой помехоустойчивых кодов, указывающей на гарантируемое число обнаруживаемых или исправляемых заданным кодом ошибок.

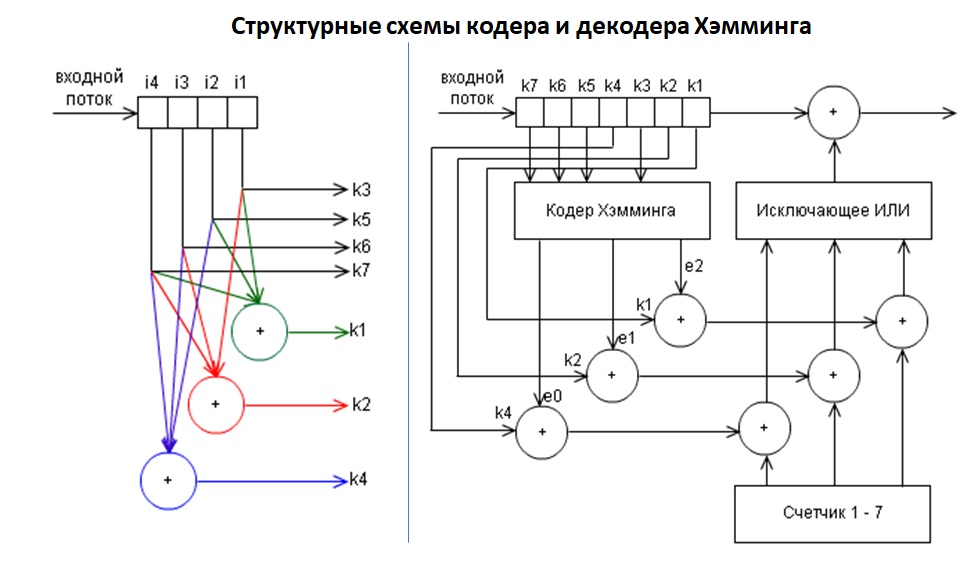


Рисунок 38 – Структурные схемы кодера и декодера Хемминга

e0,e1,e2 опрделяются как функции, зависящие от принятых декодером бит k1 — k7:

e0 = k1 + k3 + k5 + k7 mod 2

 e1 = k2 + k3 + k6 + k7 mod 2

 e2 = k4 + k5 + k6 + k7 mod 2

 Набор этих значений e2e1e0 есть двоичная запись позиции, где произошла ошибка при передаче данных. Декодер эти значения вычисляет, и если они все не равны 0 (то есть не получится 000), то исправляет ошибку.

Пример работы кодера Хэмминга (рисунок 39):

Имеется входная последовательность: 0 1 0 0 0 1 0 0   0 0 1 1 1 1 0 1 (16 бит)

Прежде всего, необходимо вставить контрольные биты. Они вставляются в строго определённых местах — это позиции с номерами, равными степеням двойки. В нашем случае это будут позиции 1, 2, 4, 8, 16. Соответственно, получилось 5 контрольных бит (выделены красным цветом):

0   0   0   0 1 0 0  0  0 1 0 0   0 0 1   0   1 1 1 0 1

Таким образом, длина всего сообщения увеличилась на 5 бит. До вычисления самих контрольных бит, мы присвоили им значение «0».

***Вычисление контрольных бит.***

 Теперь необходимо вычислить значение каждого контрольного бита. Значение каждого контрольного бита зависит от значений информационных бит, но не от всех, а только от тех, которые этот контрольных бит контролирует. Закономерность такова: контрольный бит с номером N контролирует все последующие N бит через каждые N бит, начиная с позиции N.



Рисунок 39 – Пример работы кодера Хемминга

Знаком «X» обозначены те биты, которые контролирует контрольный бит, номер которого справа. К примеру, бит номер 12 контролируется битами с номерами 4 и 8. Чтобы узнать, какими битами контролируется бит с номером N надо просто разложить N по степеням двойки.

 Вычисление значений контрольных битов: берём каждый контрольный бит и смотрим сколько среди контролируемых им битов единиц, получаем некоторое целое число и, если оно чётное, то ставим ноль (операция сложения по модулю 2), в противном случае ставим единицу.

 Высчитав контрольные биты для нашего информационного слова получаем следующее:

1 0   0   1   1 0 0  0  0 1 0 0   0 0 1   0   1 1 1 0 1

***Декодирование и исправление ошибок.***

 Допустим, закодированное первой частью алгоритма сообщение пришло с ошибкой. Например, 11-ый бит исказился:

1 0   0   1   1 0 0  0  0 1 1 0   0 0 1   0   1 1 1 0 1

Необходимо заново вычислить все контрольные биты (так же как и в первой части) и сравнить их с контрольными битами, которые мы получили. Так, посчитав контрольные биты с неправильным 11-ым битом мы получим

0 1   0   1   1 0 0  1  0 1 1 0   0 0 1   0   1 1 1 0 1

Контрольные биты под номерами: 1, 2, 8 не совпадают с такими же контрольными битами, которые мы получили. Сложив номера позиций неправильных контрольных бит (1 + 2 + 8 = 11), получаем позицию ошибочного бита.

**Классификация помехоустойчивых кодов (рисунок 40)**



Рисунок 40 - Классификация помехоустойчивых кодов

## Лекция 5.4 Методы цифровой модуляции сигналов

#### Модуляция сигналов

***Модуляция*** - это процесс преобразования одного или нескольких параметров высокочастотного несущего сигнала в соответствии с мгновенными значениями информационного низкочастотного сигнала.

Низкочастотный информационный  сигнал, по закону которого меняется высокочастотный, называется  модулирующим сигналом. Высокочастотный сигнал, являющийся несущим колебанием, называется моделируемым.

В результате модуляции низкочастотные сигналы переносятся в область более высоких частот, что позволяет:

•согласовать параметры сигнала с параметрами линии;

•повысить помехоустойчивость сигналов;

•увеличить дальность передачи сигналов;

•организовать многоканальные системы передачи.

Модуляция осуществляется в устройствах модуляторах.

*В качестве несущего сигнала может использоваться:*

•гармоническое колебание, при этом модуляция называется аналоговой или непрерывной;

•периодическая последовательность импульсов, при этом модуляция называется импульсной;

•постоянный ток, при этом модуляция называется шумоподобной.

Так как в процессе модуляции изменяются информационные параметры несущего колебания, то название вида модуляции зависит от изменяемого параметра этого колебания.

##### Цифровая модуляция (Манипуляция)

— процесс преобразования последовательности кодовых символов в последовательность элементов сигнала (частный случай модуляции — при дискретных уровнях модулирующего сигнала)

***Амплитудная манипуляция (amplitude shift keying (ASK)***— изменение сигнала, при котором скачкообразно меняется амплитуда несущего колебания (рисунок 41).

Амплитуда высокочастотного сигнала на выходе радиопередатчика принимает только два значения: включено и выключено. Огибающая радиоимпульса на практике не прямоугольная (как это показано схематично на рисунке), а имеет плавные передний и задний фронты. В противном случае частотный спектр сигнала может стать недопустимо широким, а при приёме сигнала на слух ощущаются неприятные щелчки.

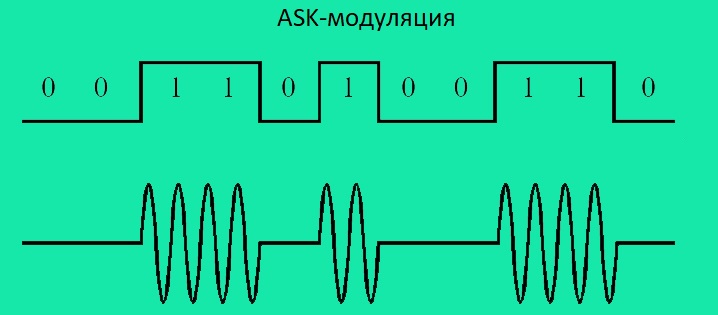
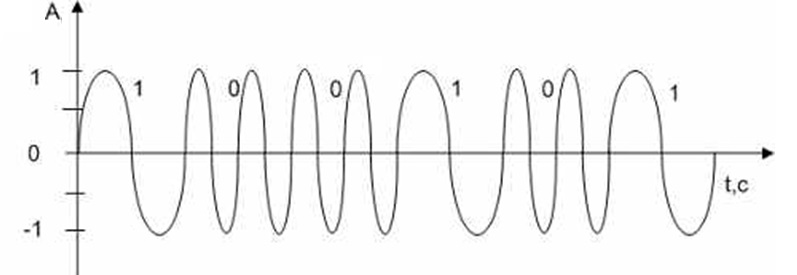


Рисунок 41 - Амплитудная манипуляция

***Частотная манипуляция (Frequency Shift Keying (FSK))***

При частотной манипуляции (ЧМн, Frequency Shift Keying (FSK)) значениям «0» и «1» информационной последовательности соответствуют определённые частоты синусоидального сигнала при неизменной амплитуде. Частотная манипуляция весьма помехоустойчива, поскольку помехи телефонного канала искажают в основном амплитуду, а не частоту сигнала. Однако при частотной манипуляции неэкономно расходуется ресурс полосы частот телефонного канала. Поэтому этот вид модуляции применяется в низкоскоростных протоколах, позволяющих осуществлять связь по каналам с низким отношением сигнал/шум (рисунок 42).



*Рисунок 42 - Частотная манипуляция*

**Фазовая манипуляция( phase-shift keying (PSK))**

— один из видов фазовой модуляции, при которой фаза несущего колебания меняется скачкообразно в зависимости от информационного сообщения (рисунок 43).

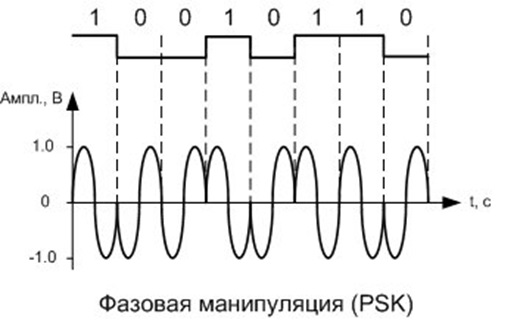


Рисунок 43 - Фазовая манипуляция

***Виды фазовой манипуляции:***

•Двоичная (BPSK) - самая простая форма фазовой манипуляции. Работа схемы двоичной ФМн заключается в смещении фазы несущего колебания на одно из двух значений, нуль или  (180°). Двоичную фазовую манипуляцию можно также рассматривать как частный случай квадратурной манипуляции (QAM-2) (рисунок 44).

•Квадратурная (QPSK)

•π/4 QPSK

•Восьмипозиционная PSK

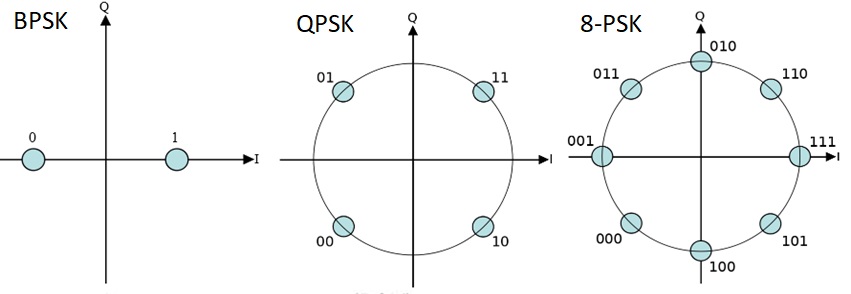


Рисунок 44 - Виды фазовой манипуляции

***Комбинации амплитудной и фазовой манипуляции (примеры: QAM16, QAM64, QAM256) – рисунок 45, 46.***

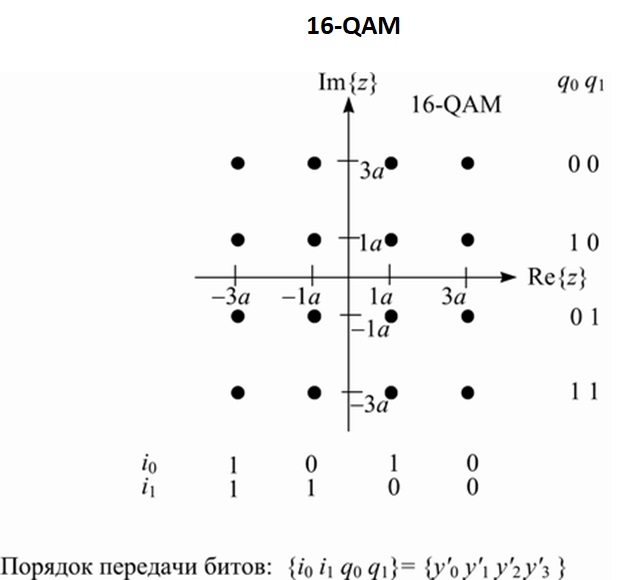


Рисунок 45 - QAM16

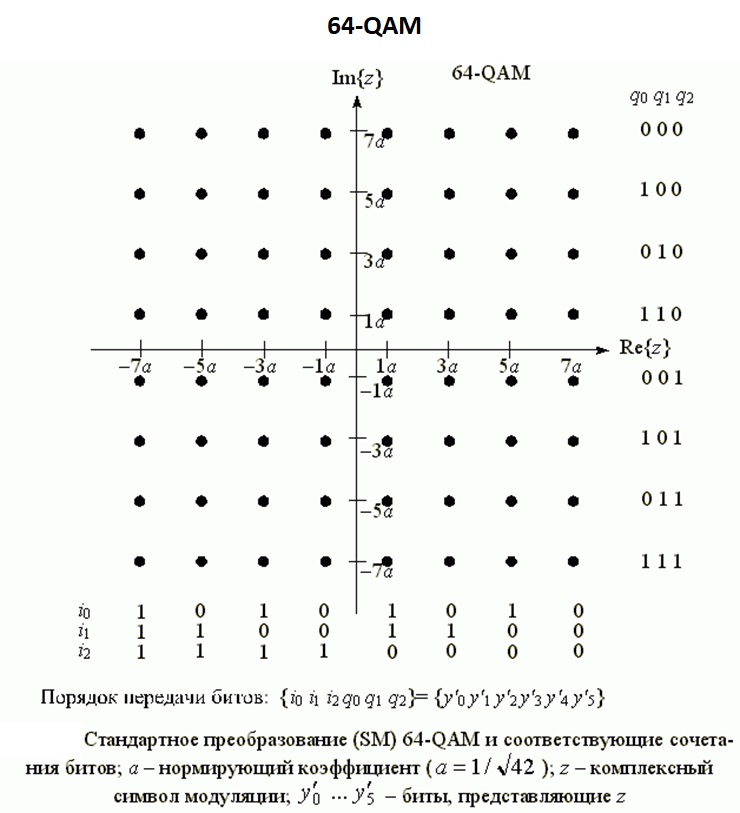


Рисунок 46 – QAM64

# Тема 6. Беспроводные телекоммуникационные сети. WLAN-сети. Проектирование сетей Wi-Fi

## Лекция 6.1 Wi-Fi. Методы высокоскоростной передачи данных. OFDM и MIMO

**Основные характеристики технологии Wi-Fi**

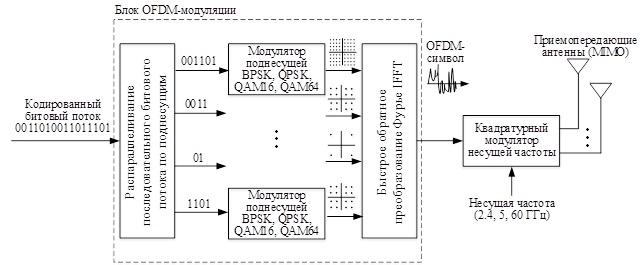
В настоящее время в связи с развитием рынка беспроводных устройств все большую популярность приобретают сети Wi-Fi (технологии на базе стандартов IEEE802.11), которые используются в качестве решений «последней мили» для организации доступа беспроводных абонентов в Интернет. Очевидными достоинствами беспроводных локальных сетей Wi-Fi (WLAN) являются мобильность абонентов, отсутствие проводов, возможность организации множественного доступа к общей радиосреде и пр. Недостатками таких систем являются низкий уровень безопасности, подверженность к радиочастотным помехам, обусловленная использованием нелицензируемых диапазонов, относительно невысокие скорости передачи данных.

Существует множество протоколов, реализованных в рамках стандарта IEEE802.11. В таблице 3 приведены некоторые характеристики существующих в настоящее время решений. Список протоколов, представленный в таблице, далеко не полон.

*Таблица 3 -* Стандарты Wi-Fi IEEE802.11

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Название | Макс. скор., Мбит/с | Модуляция | Кодирование | Технологии | Диапазон частот,ГГц |
| IEEE 802.11a | 54 | BPSK, QPSK, QAM16, QAM64 | Сверточное | OFDM | 5 |
| IEEE 802.11b | 11 | DBPSK, DQPSK | Barker11, CCK | DSSS | 2.4 |
| IEEE 802.11g | 54 | DBPSK, DQPSK | Barker11, CCK | DSSS, OFDM | 2.4 |
| IEEE 802.11n | 600 | BPSK, QPSK, QAM16, QAM64 | Сверточное | OFDM, MIMO4x4, MU-MIMO | 2.4, 5 |
| IEEE802.11ad | 6930 | BPSK, QPSK, QAM16, QAM64, QAM256 | Сверточное | OFDM, MIMO8x8, MU-MIMO | 2.4, 5, 60 |
| IEEE 802.11s | 54 | BPSK, QPSK, QAM16, QAM64 | Сверточное | Wireless Mesh,OFDM | 2.4, 5 |
| IEEE802.11ac | 6930 | BPSK, QPSK, QAM16, QAM64, QAM256 | Сверточное | OFDM, MIMO8x8, MU-MIMO, WAVE | 5 |

На рисунке 47 представлена общая структура передатчика Wi-Fi на базе OFDM-модулятора с поддержкой MIMO. Битовый поток, предварительно закодированный и зашифрованный (опционально) подается на логический блок, который распараллеливает его по имеющимся поднесущим частотам. Число поднесущих зависит от ширины полосы частот (20 или 40 МГц), а также от версии протокола. В рамках данной лабораторной работы мы сосредоточим внимание на наиболее используемом в настоящее время решении – IEEE802.11n. Для Wi-Fi на базе IEEE802.11n в 20 МГц число поднесущих в 20 МГц полосы равно 56.



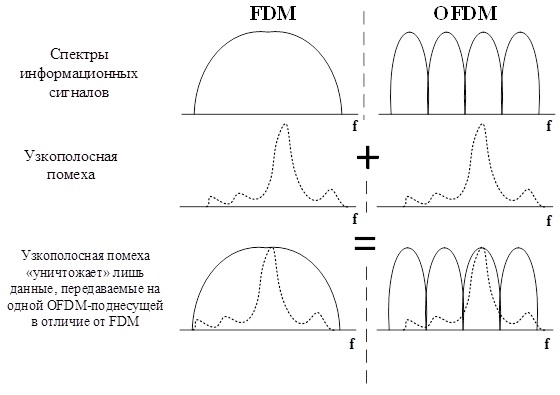
*Рисунок 47 -* Общая схема OFDM-передатчика Wi-Fi с поддержкой MIMO.

Каждая поднесущая модулируется отдельным BPSK-/QPSK-/QAM16-/QAM64-модулятором в зависимости от текущих радиоусловий. После этой промежуточной модуляции данные с каждой поднесущей подаются на блок обратного преобразования Фурье (IFFT), где они суммируются и умножаются на определенную промежуточную частоту. В результате на выходе блока IFFT получается временн*о*е представление сигнала или OFDM-символ, который затем модулирует несущую частоту в блоке квадратурного модулятора и предается на антенну (или антенны в случае MIMO) и отправляется на радиоинтерфейс.

На приемной стороне (не показано на рисунке 47) происходит все то же самое только в обратном направлении (прием сигнала, демодуляция, прямое преобразование Фурье и пр.).

Рассмотрим ключевые технологии, направленные на увеличение спектральной эффективности сетей Wi-Fi. Прежде всего – это OFDM – мультиплексирование поднесущих частот с ортогональным частотным разделением. В настоящее время данная технология формирования радиосигнала используется в самых разных телекоммуникационных системах – WIMAX, LTE, LTE-Advanced, DVB-T и пр. Основными достоинствами, сделавшими OFDM настолько часто используемым решением, являются адаптивность к частотно-селективным помехам (узкополосные помехи, наиболее часто встречающиеся в городских радиоусловиях, обусловленные многолучевым распространением сигналов) и относительная простота реализации. На рисунке 48 показано влияние частотно-селективных помех на FDM и OFDMсигналы.

Очевидно, что при реализации OFDM, у системы есть возможность адаптироваться к помехе путем, например, выбора более помехоустойчивых схем модуляции и кодирования для поднесущих, подверженных помехам, в отличие от FDM-сигнала, который полностью «уничтожается» узкополосной помехой.



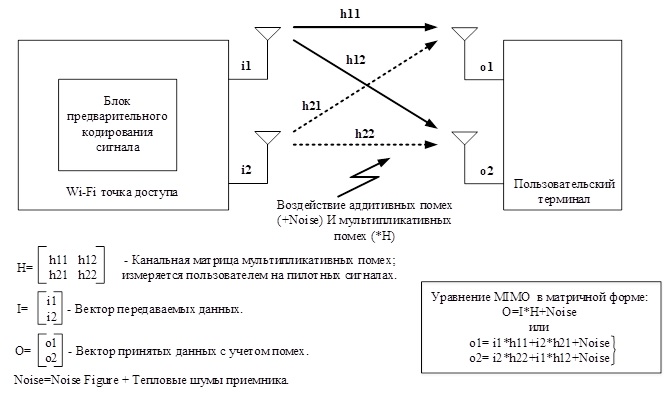
*Рисунок 48 -* Сравнение OFDM и FDM.

Есть хорошая аналогия, позволяющая наглядно увидеть отличия между OFDM и FDM: FDM можно сравнить с потоком воды (поток данных), текущим из крана, в то время как OFDM – это поток воды той же интенсивности, но текущий из лейки душа отдельными струйками (поднесущие). Если заткнуть пальцем кран (аналог частотно-селективной помехи), то можно перекрыть весь поток воды. Перекрыть же одним пальцем все струйки, текущие из душа, вряд ли удастся. Таким образом, даже несмотря на воздействие помех, OFDM-технология позволяет передавать данные со скоростью б*о*льшей, чем классическое FDM-решение

Еще одной немаловажной технологией, применяемой в Wi-Fi для увеличения скорости передачи данных, является MIMO (Multiple Input Multiple Output). Основная идея заключается в том, что данные распределяются по нескольким передающим (Input) антеннам и передаются одновременно в одной и той же полосе частот. Чтобы понять, как декодируются данные передаваемые в одно и тоже время в одной и той же полосе частот без применения кодового разделения, рассмотрим рисунок 49.

На две передающие антенны Wi-Fi точки доступа (input) подаются два потока данных, которые затем направляются в радиоканал. Представим данные, передаваемые от точки доступа в нисходящем к пользователю канале (DL – Downlink) в виде вектора *I*, имеющего два значения: *i1* – данные, передаваемые первой антенной и *i2* – данные, передаваемые второй антенной.

*Рисунок 49 -* Реализация MIMO в беспроводных сетях.



При прохождении через радиоканал данные вектора *I* подвергаются воздействию двух типов помех – аддитивным и мультипликативным. Аддитивные помехи, как правило, постоянны и состоят из тепловых шумов приемника (*ThermalNoise*), зависящих от ширины полосы частот сигнала, и из коэффициента шума усилителя (*Noise Figure*), зависящего от реализации приемо-передающего оборудования конкретным производителем оборудования. Мультипликативные же помехи носят переменный характер и во многом обусловлены наличием переотражений сигналов в радиоканале, многолучевым распространением сигнала, и измеряются пользователем на специальных опорных (или пилотных) сигналах. Результаты таких измерений заносятся в канальную матрицу *H*.

Таким образом, результирующий сигнал на входе приемника пользовательского оборудования O (Output) в матричной форме будет иметь вид:

O=I\*H+Noise,                                     (3)

где *Noise* – это аддитивные шумы приемника. Для того чтобы успешно решить систему уравнений (3) и определить, какие же данные были переданы пользователю, требуется гарантировать, что уравнения, входящие в систему, были линейно независимы. Должной степени линейной независимости между уравнениями можно добиться путем пространственного разнесения передающих антенн, а также при условии, что сигнал проходит через среду, несколькими путями (многолучевое распространение). Но говоря о сетях Wi-Fi, мы говорим о совсем небольшом радиопокрытии (несколько десятков метров), где сложно обеспечить многолучевость. Для того чтобы привнести искусственно линейную независимость в систему уравнений (3) на стороне передатчика реализуется специальный блок предварительного кодирования сигналов, изменяющий по определенным правилам, описанных стандартом, фазы и амплитуды передаваемых сигналов.

         MIMO может работать в нескольких режимах. Прежде всего – это режим пространственного мультиплексирования данных, при котором каждая антенна передает отдельный поток данных, увеличивая пропускную способность. Однако, при ухудшении радиоусловий, обе антенны могут дублировать передачу одного потока данных, улучшая помехозащищенность.

         На рисунке 3 показан пример, когда данные с обеих передающих антенн предназначены одному пользователю – это пример режима Single User MIMO (SU-MIMO). Возможна также реализация режима Multi User MIMO (MU-MIMO), когда Wi-Fi точка доступа передает потоки данных, предназначенные разным конечным пользователям, увеличивая емкость сети.

         Более подробно познакомиться с основными особенностями и технологиями, используемыми в Wi-Fi сетях, можно в [5-6].

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9 (12)

[6] Шахнович, И. Современные технологии беспроводной связи [Текст] : монография / И. Шахнович. - М. : Техносфера, 2004. - 166с. (9)

[7] Попов, В. И. Основы сотовой связи стандарта GSM [Текст] : монография / В. И. Попов. - М. : Эко-Трендз, 2005. - 292с.

[8] Сети UMTS. Архитектура, мобильность, сервисы [Текст] : монография / Х.Кааранен, А. Ахтиайнен, Л. Лаитинен и др.; пер. с англ. Н.Л. Бирюкова. - М. : Техносфера, 2007. - 458с. (7)

[9]    Тихвинский, В. О. Сети мобильной связи LTE: Технологии и архитектура [Текст] : монография / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. - М. : Эко-Трендз, 2010. - 283с.

## Лекция 6.2 Особенности проектирования радиопокрытия локальных беспроводных сетей Wi-Fi (WLAN)

**Особенности проектирования радиопокрытия локальных беспроводных сетей Wi-Fi (WLAN)**

В рамках данной лабораторной работы нас будут интересовать принципы расчета радиуса действия точки доступа Wi-Fi (IEEE 802.11n). Для того чтобы оценить радиопокрытие любой беспроводной точки доступа, необходимо понимать, какие существуют физические факторы, ограничивающие зону действия радиосигналов. Прежде всего, это чувствительность приемного устройства *RxSens* (точки доступа или пользовательского терминала), которая рассчитывается как:

RxSens=NoiseFigure+ThermalNoise+RequiredSINR,    (4)

где *NoiseFigure* – коэффициент шума, задаваемый производителем оборудования; *RequiredSINR* – требуемое отношение мощности сигнала к мощности шумов и интерференции, зависящее от используемых схем модуляции и кодирования MCS; *ThermalNoise* – тепловой шум приемника, определяемый по формуле:

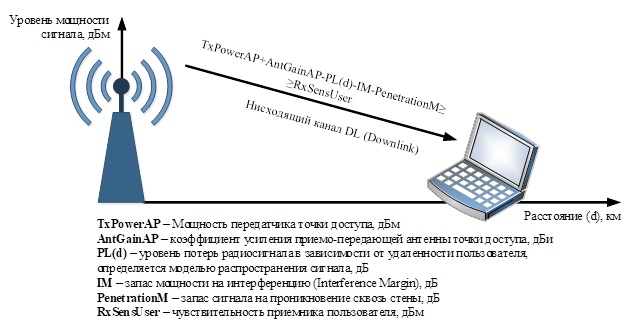
ThermalNoise=-174+10log10(BW),         (5)

где *BW* – ширина полосы частот принимаемого сигнала в Гц, а -174 дБм – уровень шума на 1 Гц полосы частот при температуре 200С.

         Таким образом, значение, получаемое из выражения (4) – это минимальный требуемый уровень радиосигнала, при котором возможно успешное декодирование данных. Следующий возникающий вопрос – какой же должен быть максимальный уровень допустимых потерь радиосигнала MAPL (Maximum Allowed Path loss), при котором все еще будет возможно успешное декодирование данных? Для того чтобы ответить на этот вопрос, составляется и рассчитывается так называемый бюджет восходящего (от пользователя к точке доступа UL) и нисходящего (от точки доступа к пользователю DL) каналов.

***а) Бюджет нисходящего канала (DL Link Budget)***

         На рисунке 1 представлены основные составляющие бюджета нисходящего канала DL.



*Рисунок 50* - Бюджет нисходящего канала DL Wi-Fi-сети

         В неравенстве, показанном на рисунке 50, все входные параметры за исключением *PL(d)* являются константами. В левой части этого неравенства стоят составляющие, характеризующие реальный уровень сигнала в зависимости от расстояния *d*, в правой же – требования к уровню такого сигнала, при котором декодирование будет осуществимо. Если приравнять левую и правую часть неравенства, мы получим уравнение (6), где *PL(d)* можно заменить на *MAPL\_DL* – уже независящие от расстояния максимально допустимые потери радиосигнала, которые удовлетворяют минимальным требования успешного приема данных.

TxPowerAP+AntGain-MAPL\_DL-IM-PenetrationM=RxSensUser.   (6)

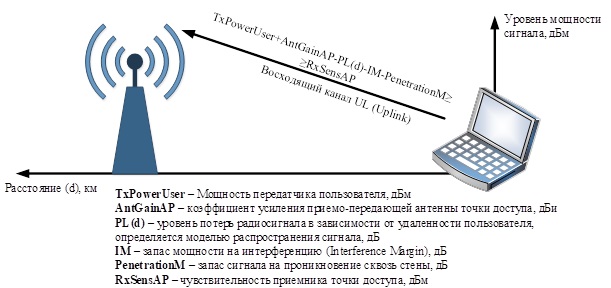
         Стоит обратить внимание на то, что результатом решения уравнения (6) будет определение допустимых потерь *MAPL\_DL* в нисходящем канале, но расстояние, на котором сигнал настолько затухнет все еще неизвестно.

***б) Бюджет восходящего канала (UL Link Budget)***

         На рисунке 51 представлены основные составляющие бюджета восходящего канала UL.

         В неравенстве, представленном на рисунке 2, все входные параметры за исключением *PL(d)* – константы. В левой части этого неравенства стоят составляющие, отражающие реальный уровень сигнала на некотором расстоянии *d* от пользователя, в правой же находятся требования к уровню такого радиосигнала, при котором декодирование будет возможно. Приравняв левую и правую часть неравенства, получаем уравнение (7), где *PL(d)*можно заменить на *MAPL\_UL* – это независящие от расстояния максимально допустимые потери радиосигнала в восходящем канале UL, которые удовлетворяют минимальным требования успешного приема данных.

TxPowerUser+AntGainAP-MAPL\_UL-IM-PenetrationM=RxSensAP.   (7)



*Рисунок 51 -* Бюджет нисходящего канала UL Wi-Fi-сети

Результатом решения уравнения (7) будет определение допустимых потерь *MAPL\_UL* в восходящем канале UL, однако расстояние, на котором сигнал затухнет на эту величину все еще неизвестно.

**в) Модели распространения сигналов в сетях Wi-Fi**

         После определения величины максимально допустимых потерь в обоих направлениях (*MAPL\_UL* и *MAPL\_DL*) возникает задача определения, на какой же удаленности от радиопередатчика *d* следует ожидать такого уровня потерь сигнала *PL*. Для решения этой задачи применяются различные модели, предсказывающие затухание радиосигнала на определенном расстоянии для самых различных радиоусловий. Такие модели бывают аналитические, например, модель свободного пространства, не учитывающая факторы воздействия внешней среды на сигнал, и эмпирические, полученные опытным путем для самых разных условий и типов приемопередающих устройств (например, модели Walfish-Iekigami, Knife-Edge, Okumura, Hata, и пр.).

         Рассмотрим две наиболее часто используемые модели распространения сигналов для точек доступа Wi-Fi, которые, как правило, устанавливаются либо в квартирах, либо в бизнес-центрах, аэропортах – модель свободного пространства FSPM (Free Space Propagation Model) и модель, учитывающую особенности функционирования точки доступа в городских радиоусловиях UMiNLOS (Urban Micro Non-Line-of-Sight).

**Модель свободного пространства FSPM**

Данная модель применяется в условиях открытого пространства между приемником и передатчиком для диапазона сверхвысоких частот (3..30 ГГц).

Формула для расчета затуханий имеет вид (8):

PL(d)=20log10(d)+20log10(f)-27.55, (8)

 где *f* – это несущая частота сигнала в МГц, *d* – расстояние между приемником и передатчиком в м.

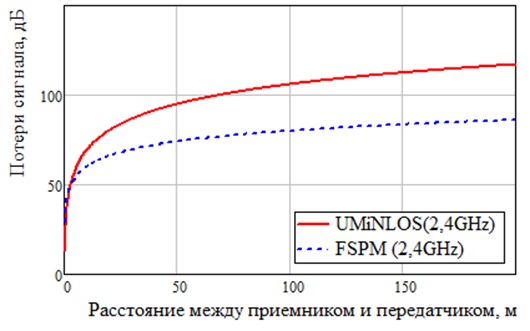
**Модель UMiNLOS**

Данная модель применяется в условиях размещения точек доступа в помещениях (Indoor).

Формула для расчета затуханий имеет вид (9):

PL(d)=26log10(f[ГГц])+22.7+36.7log10(d[м]),        (9)

На рисунке 52 представлена полученная зависимость потерь мощности радиосигнала от расстояния между приемником и передатчиком.



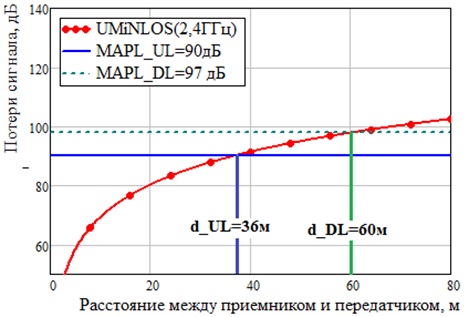
*Рисунок 52 -* Бюджет нисходящего канала UL Wi-Fi-сети

**г) Расчет радиуса действия точки доступа (Range calculation)**

         Подобрав подходящую модель распространения радиосигнала, мы получили зависимость, наглядно демонстрирующую, как затухает сигнал при увеличении расстояния между пользователем и точкой доступа Wi-Fi. Но чтобы определить, на каком же расстоянии декодирование данных будет все еще возможно, нужно знать уровень максимально допустимых потерь в обоих направлениях (*MAPL\_UL* и *MAPL\_DL*).

         Зная значения потерь радиосигнала в нисходящем и восходящем каналах, можно отложить эти величины на графике зависимости потерь сигнала от расстояния между пользователем и точкой доступа, как показано на рисунке 53. Точки пересечения *MAPL\_UL* и *MAPL\_DL*с кривой *PL(d)* покажут радиусы сети в UL и DL направлениях (*d\_UL* и *d\_DL*).

         При проектировании радиопокрытия всегда берется меньшая из величин *d\_UL* и *d\_DL,* в нашем случае – это *d\_UL*.



*Рисунок 53 -* Определение радиуса UL и DL в Wi-Fi-сети

Таким образом, используя модель распространения сигнала UMiNLOS, и рассчитав максимально допустимые потери сигнала в обоих направлениях, мы получили радиус в восходящем канале 36 м и в нисходящем канале 60 м. В результате, зона действия точки доступа Wi-Fi ограничена радиусом 36 м.

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9 (12)

[6] Шахнович, И. Современные технологии беспроводной связи [Текст] : монография / И. Шахнович. - М. : Техносфера, 2004. - 166с. (9)

[7] Попов, В. И. Основы сотовой связи стандарта GSM [Текст] : монография / В. И. Попов. - М. : Эко-Трендз, 2005. - 292с.

[8] Сети UMTS. Архитектура, мобильность, сервисы [Текст] : монография / Х.Кааранен, А. Ахтиайнен, Л. Лаитинен и др.; пер. с англ. Н.Л. Бирюкова. - М. : Техносфера, 2007. - 458с. (7)

[9]    Тихвинский, В. О. Сети мобильной связи LTE: Технологии и архитектура [Текст] : монография / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. - М. : Эко-Трендз, 2010. - 283с.

## Лекция 6.3 Основные понятия мобильных телекоммуникаций. Основы сетей 2G (GSM)

**Мобильные сети** – это интенсивно развивающиеся системы, пользующиеся огромной популярностью среди пользователей по всему миру. Очевидными преимуществами мобильных сетей перед любыми другими телекоммуникационными система является возможность организовать непрерывное обслуживание абонентов по всему миру. Две ключевые процедуры делают такую мобильность возможной:

1)               **Хэндовер** – буквально – это эстафетная передача. Хэндовер подразумевает автоматическое переключение абонента между обслуживающими станциями БС (базовые станции) при его перемещении в пространстве без перерыва сервиса, ощутимого абонентом.

2)               **Роуминг** – это соглашение между операторами мобильной связи различных регионов или стран о возможности абонентов одного оператора пользоваться инфраструктурой сети другого оператора и наоборот. То есть оператору мобильной связи не нужно строить сеть по всему миру, чтобы обеспечить своих абонентов повсеместной связью, достаточно лишь заключить роуминговое соглашение с оператором, присутствующем в другом регионе.

Кроме того, в мобильных сетях необходимо обеспечить высокий уровень безопасности, онлайн тарификацию, переключение (хэндовер) не только между базовыми станциями одного поколения, но и между различными технологиями (например, переключить абонента с сети GSM на сеть LTE).

Мобильные сети эволюционируют из года в год, видоизменяя архитектуру, технологии радиоинтерфейса и сервисы. Одно поколение G (Generation) сменяет другое. В настоящее время в коммерческом использовании операторов сотовой связи находятся сети трех поколений: 2G (GSM), 3G (WCDMA или UMTS) и 4G (LTE, LTE-Advanced). Основные отличия между технологиями 1, 2, 3 и 4-го поколений представлены в таблице 4.

*Таблица 4 -* Четыре поколения мобильной связи

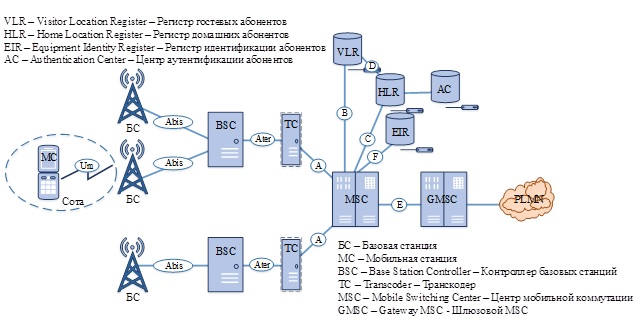
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Характеристика | **1G** | **2G** | **3G** | **4G** |
| **Виды сигналов** | Аналоговые | Цифровые | Цифровые | Цифровые |
| **Названия стандартов** | AMPS, TACS, NMT, Radiocom2000, NTT, C-450 | D-AMPS, TDMA, CDMA, GSM, PDC | WCDMA, CDMA2000, UMTS | WIMAX, LTE, LTE-Advanced |
| **Год появления** | 1984 | 1991 | 2006-2007 | 2008-2010 |
| **Методы разделения ресурсов** | FDMA | FDMA+TDMA, CDMA | CDMA | OFDMA, SC-FDMA |
| **Ключевые особенности, сервисы** | Голосовые сервисы, частотно-территориальное планирование | Голос, передача SMS,  частотно-территориальное планирование | Голос, SMS, мультимедиа MIMO, IMS, кодовое планирование | Голос по IP, SMS, мультимедиа MIMO, Carrier aggregation, CoMP, SON, All-IP архитектура, IMS  и пр. |
| **Технологии и скорости передачи данных** | - | GPRS, EDGE  До 384 кбит/с | HSDPA, HSUPA, HSPA, HSPA+  До 42 Мбит/с | WIMAX, LTE, LTE-Advanced  100Мбит/с – 1.5 Гбит/с |

Рассмотрим ключевые особенности технологий мобильной связи 2-4-го поколений, которые оказывают существенное влияние на емкость и спектральную эффективность таких сетей. Все эти технологии поддерживают различные методы передачи данных, однако, в рамках данной лабораторной работы, мы будем оценивать такой критерий эффективности как количество голосовых абонентов на одну односекторную базовую станцию.

**Мобильные сети 2-го поколения GSM**

В данном разделе мы рассмотрим самые основные особенности сетей 2-го поколения. Чтобы получить более глубокое представление о таких сетях рекомендуется ознакомиться с [7].

Архитектура мобильных сетей GSM представлена на рисунке 54.

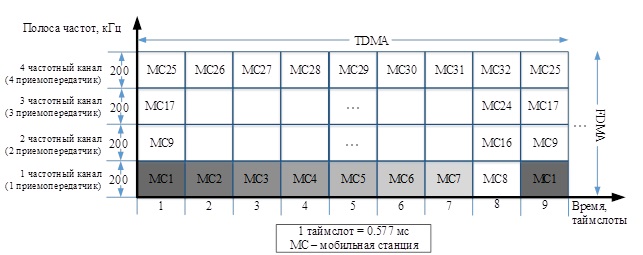


*Рисунок 54 -* Архитектура сети GSM

Радиоподсистема GSM состоит из БС (Базовая станция), контроллеров БС BSC и транскодеров. БС выполняют функции приемо-передатчиков сигналов, в то время как вся обработка данных и управление радиоресурсами осуществляется контроллером BSC. Одной из важнейших задач BSC, в частности, является управление хэндоверами МС. Перед отправкой данных в транспортную сеть транскодер TC выполняет перекодировку данных из формата GSMв стандартные форматы голосовой телефонии. Затем данные направляются на MSC и GMSC, которые по сути не участвуют в обработке данных, выполняя лишь функции, связанные с авторизацией пользователей за счет наличия доступа к различным базам данных (HLR, VLR, EIR, AC). Как мы увидим уже в сетях 3-го поколения прекратится передача голосового и прочего трафика через MSC.

MSC – пожалуй, важнейший элемент сети WCDMA (центр мобильной коммутации). Именно MSC отвечает за коммутацию голосовых каналов для своих абонентов. Кроме того, в сетях 2G MSC собирает данные по биллингу пользователей.

Абоненты (МС) в сетях GSM получают фиксированные по времени (TDMA) и по частоте (FDMA) ресурсы как показано на рисунке 55. Каждый частотный канал шириной 200 кГц закрепляется за отдельным приемопередатчиком БС. Важно, что в GSM, в отличие от сетей первого поколения, частотный канал выделяется абоненту не на все время активного соединения, а лишь в каждый предопределенный интервал времени, называемый таймслот.



*Рисунок 55 -* Частотно-временное распределение ресурсов в сетях GSM

           Вся ось времени делится на таймслоты длительностью 0.577 мс. Абонентам при установлении соединения назначается каждый 8-й таймслот в восходящем и нисходящем каналах. Таймслоты, предназначенные для передачи пользовательских данных называются каналами трафика, остальные же таймслоты, используемые сетью для контроля радиоинтерфейса – каналами управления. Если на базовой станции всего один приемопередатчик (т.е., всего один частотный канал), то из 8 имеющихся временных физических каналов как минимум один будет занят данными логических каналов управления. Как правило, операторы мобильной связи имеют 4 приемопередатчика для организации радиопокрытия и обеспечения емкости в одной соте. При такой конфигурации число физических каналов будет равно 4х8=32, из которых минимум два отдаются под логические каналы управления, остальные же 30 могут быть задействованы как логические каналы трафика.

Для расчета количества абонентов, которое БС сможет обслуживать в ЧНН, используется формулу Эрланга:

* Число каналов управления на одной БС;
* *Pblock* - Вероятность отказа в установлении соединения абонента;
* *G* - Интенсивность нагрузки одного абонента в ЧНН (Час Наибольшей Нагрузки).

Зная значение суммарной нагрузки G и нагрузки, генерируемой одним абонентом g, несложно определить, что число абонентов N2, которое может обслужить одна БС равно:

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9 (12)

[6] Шахнович, И. Современные технологии беспроводной связи [Текст] : монография / И. Шахнович. - М. : Техносфера, 2004. - 166с. (9)

[7] Попов, В. И. Основы сотовой связи стандарта GSM [Текст] : монография / В. И. Попов. - М. : Эко-Трендз, 2005. - 292с.

[8] Сети UMTS. Архитектура, мобильность, сервисы [Текст] : монография / Х.Кааранен, А. Ахтиайнен, Л. Лаитинен и др.; пер. с англ. Н.Л. Бирюкова. - М. : Техносфера, 2007. - 458с. (7)

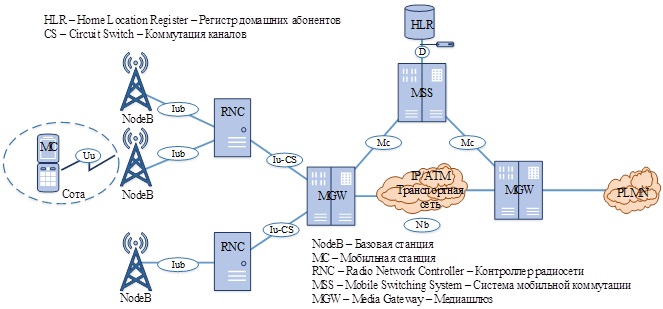
[9]    Тихвинский, В. О. Сети мобильной связи LTE: Технологии и архитектура [Текст] : монография / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. - М. : Эко-Трендз, 2010. - 283с.

**Лекция 6.4 Основы сетей 3G (WCDMA)**

**Мобильные сети 3-го поколения WCDMA**

В данном разделе будут рассмотрены лишь основные особенности сетей 3-го поколения. Чтобы получить более детальное представление об этих сетях рекомендуется ознакомиться с [8].

Архитектура мобильных сетей WCDMA представлена на рисунке 56.



*Рисунок 56 -* Архитектура сети WCDMA

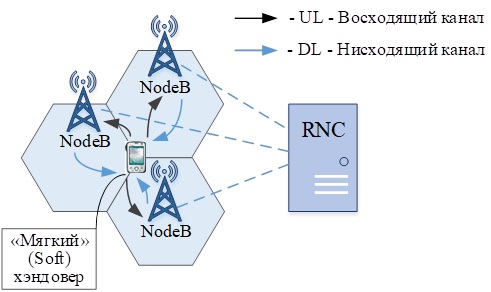
Стоит отметить, принципиальные архитектурные отличия сетей 3-го поколения по сравнению с сетями GSM – исчез транскодер и появился медиашлюз MGW. Функции транскодирования взял на себя контроллер радиосети RNC. Основное же назначение MGW – это передача трафика абонентов. Этот элемент не обладает какими-либо управляющими полномочиями. Задачей такого решения было разгрузить MSS, сделать его исключительно сигнальным элементом сети, отвечающим за все процедуры, подразумевающие авторизацию абонентов, а также снизить стоимость транспортных каналов.

Для разделения трафика различных пользователей в сетях 3G WCDMA (или UMTS) используются специальные ортогональные последовательности, например, функции Уолша. Такой метод разделения ресурсов называется CDMA (Code Division Multiple Access – множественный доступ с кодовым разделением). Для того чтобы понять, как это работает, достаточно представить комнату, в которой находятся несколько человек, говорящих на разных языках одновременно. Входя в комнату, вы слышите их всех, но не можете понять, что именно говорят, например, ребята по-японски, так как вы не знаете этот язык (ортогональный код). Услышав же знакомое слово по-русски, вы с большой вероятностью успешно его «декодируете», несмотря на некоторый уровень шума голосов в комнате. Именно так работает CDMA. Базовая станция находит своих абонентов (а абоненты – базовую станцию) по ортогональному коду. Однако тут очевидна проблема, если число одновременно говорящих в соте (комнате) абонентов превышает некоторый порог (порог слышимости), то из-за слишком высокого уровня шума их сигналы становятся неразличимы. Это называется шумом внутри соты.

Кроме того, сети WCDMA подвержены влиянию интерференции, от соседних сот, так как в таких сетях не предусмотрено частотное разделение между соседними сотами – все соты сети работают на одной и той же частоте.

Теоретически, благодаря ортогональности каналообразующих кодов, интерференция внутри соты должна быть равна нулю. Но из-за многолучевого распространения сигналов, вызванного переотражениями, может нарушаться ортогональность. При расчете абонентской емкости это учитывается путем введения коэффициента ортогональности кода α, принимающего значения от 0 до 1 в зависимости от условий распространения сигнала.

Для улучшения производительности взаимодействия между базовыми станциями NodeB и абонентами в 3Gподдерживается особый вид хэндовера – «мягкий» (soft) хэндовер (рисунок 57). Такой вид хэндовера реализован только в сетях 3-го поколения WCDMA.



*Рисунок 57 -* Soft-хэндовер в сети WCDMA

Особенность «мягкого» хэндовера заключается в том, что абонент, находящийся на границе нескольких сот, принадлежащих одной или нескольким базовым станциям, может обслуживаться ими одновременно – принимать и передавать данные. Это возможно при условии, что все базовые станции подключены к общему контроллеру радио сети RNC, который выполняет обработку пользовательских данных. Очевидно, что необходимость дублировать данные на нескольких сотах (по стандарту до 6, на практике – 2-3 соты) приводит к увеличению ресурсных затрат. При расчете абонентской емкости это учитывается с помощью параметра *SHOOH*.

Для расчета количества голосовых абонентов, которое БС сможет обслуживать в ЧНН, используется формулу:

Описание переменных для расчета абонентской емкости сетей 3G:

* Скорость передачи данных для голосовых услуг *R*;
* Требуемое отношение сигнал/шум для голоса *E/N*;
* Чиповая скорость в WCDMA (UMTS) *W*;
* Коэффициент ортогональности кода α;
* Коэффициент интерференции по соседней соте *i* для сот со всенаправленной антенной;
* Затраты ресурсов на мягкий хэндовер *SHOOH*;
* Коэффициент загрузки нисходящего канала *ηDL*;
* Коэффициент активности абонента *u*.

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9 (12)

[6] Шахнович, И. Современные технологии беспроводной связи [Текст] : монография / И. Шахнович. - М. : Техносфера, 2004. - 166с. (9)

[7] Попов, В. И. Основы сотовой связи стандарта GSM [Текст] : монография / В. И. Попов. - М. : Эко-Трендз, 2005. - 292с.

[8] Сети UMTS. Архитектура, мобильность, сервисы [Текст] : монография / Х.Кааранен, А. Ахтиайнен, Л. Лаитинен и др.; пер. с англ. Н.Л. Бирюкова. - М. : Техносфера, 2007. - 458с. (7)

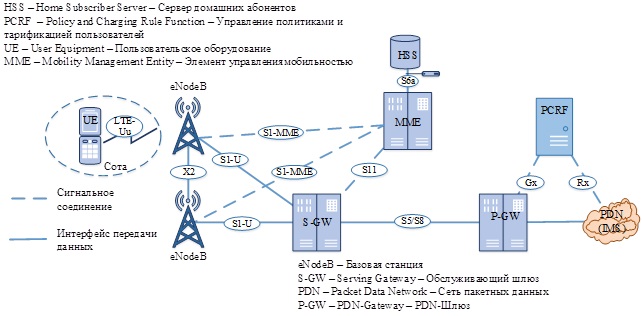
[9]    Тихвинский, В. О. Сети мобильной связи LTE: Технологии и архитектура [Текст] : монография / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. - М. : Эко-Трендз, 2010. - 283с.

## Лекция 6.5 Основы сетей 4G (LTE, LTE-Advanced)

**Мобильные сети 4-го поколения LTE**

В данном разделе мы рассмотрим лишь некоторые особенности сетей 4-го поколения. Чтобы получить более глубокое представление о таких сетях рекомендуется ознакомиться с [9].

На рисунке 58 представлена архитектура мобильных сетей LTE. Пунктирными линиями показаны исключительно сигнальные интерфейсы для обмена управляющими сообщениями. Сплошные линии – это интерфейсы передачи пользовательских данных. Стоит отметить, что архитектура сетей 4-го поколения не подразумевает наличие централизованного управления радиоподсистемой, то есть здесь отсутствует контроллер базовых станций eNodeB. Но для обеспечения взаимодействия между eNodeB здесь появляется логический интерфейс X2. Базовые станцииeNodeB отвечают за выполнение всех функций, связанных с управлением радиоресурсами (динамическое распределение ресурсов, шифрование данных, HARQ, управление QoS, MIMO и пр.).



*Рисунок 58 -* Архитектура сети LTE

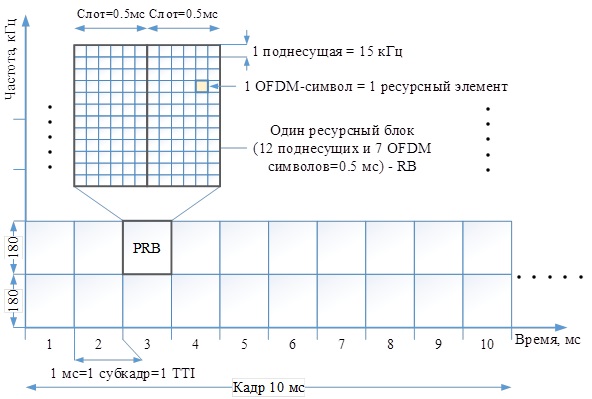
«Мозгом» сети LTE является элемент управления мобильностью MME, который имеет доступ к данным из HSS для выполнения всех процедур, подразумевающих необходимость авторизации UE (МС) – установление и управление соединениями, регистрация в сети, обновление местоположение и пр. Кроме того, MME по интерфейсу S11 осуществляет управление S-GW и P-GW для организации логических транспортных каналов передачи данных.

Основной функцией P-GW является назначение IP-адресов для пользовательских сессий. Помимо этого, P-GWпринимает участие в управлении качеством обслуживания и тарификациями совместно с PCRF.

Важно отметить, что все интерфейсы сети LTE – это IP-интерфейсы. Это означает, что организация голосового трафика возможна только с использованием технологий VoIP и при наличии подключения к сети IMS.

Одной из ключевых особенностей LTE, делающих эту технологию столь популярной среди операторов всего мира – это поддержка частотного (FDD) и временного (TDD) режимов дуплексирования восходящего и нисходящего каналов. При FDD требуются две отдельные полосы частот для UL и DL направлений, в то время как в режиме TDD передача в обоих направлениях осуществляется в одной полосе частот, которая определенным образом во времени распределена между ними в зависимости от величины загрузки UL и DL. К достоинствам FDD по сравнению с TDDможно отнести высокую пропускную способность в восходящем и нисходящем каналах, а к недостаткам – неэффективное использование полосы частот восходящего канала, необходимость иметь лицензии на спаренные частоты, дорогие дуплексные фильтры.

На рисунке 59 показана частотно-временная структура радиоинтерфейса LTE в режиме FDD. Вся ось времени разбита на кадры длительностью 10 мс, каждый из которых в свою очередь делится на 10 субкадров по 1 мс или TTI (Time Transmission Interval). Каждый TTI состоит из 2 слотов по 0,5 мс. Одним ресурсным блоком RB (Resource Block) называется совокупность 7 OFDM-символов (или ресурсных элементов) при условии, что используется нормальный, а не расширенный циклический префикс (встроенный LTE-механизм для борьбы с межсимвольной интерференцией, вызванной многолучевым распространением сигнала), и 12 ортогональных поднесущих с разносом по частоте в 15 кГц.

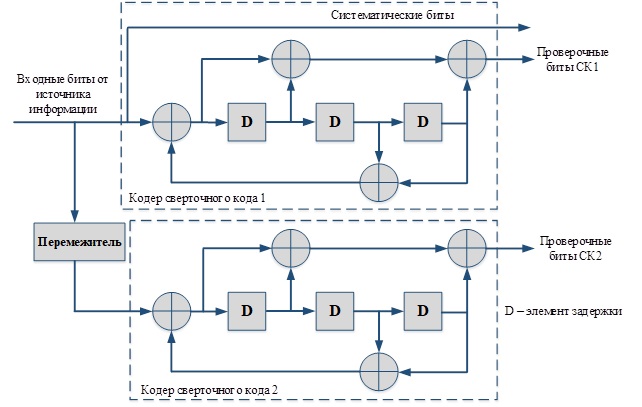


*Рисунок 59* - Частотно-временная структура радиоинтерфейса LTE (FDD)

Два последовательных по времени ресурсных блока называются физическим ресурсным блоком PRB (Physical Resource Block) и являются минимальной порцией ресурса, выделяемого абоненту в случае необходимости.

Для обеспечения помехозащищенности данных каждый транспортный блок данных вместе с битами контрольной суммы предварительно подвергается турбо кодированию, схема которого показана на рисунке 60.

Контрольная сумма или CRC (Cyclic Redundancy Check) используется в LTE для определения успешности декодирования транспортного блока в рамках механизма HARQ. В случае невозможности правильно декодировать блок данных отправляется отрицательная квитанция, в ответ на которую повторно пересылается блок данных с б*о*льшим числом избыточных (проверочных) битов.



*Рисунок 60 -* Схема реализации турбо-кодера в LTE

Как было показано на рисунке 16, каждый ресурсный элемент (или OFDM-символ модулируется и защищается помехоустойчивым кодированием в зависимости от качества радиоканала CQI (Channel Quality Indicator). Сочетание метода модуляции и кодирования называется MCS (Modulation and Coding Scheme) и определяет спектральную эффективность символа. Например, если используется MCS=QPSK1/3, то количество информационных бит, передаваемых за секунду в 1 Гц полосы (или в одном OFDM-символе), определяется как 2(*модуляция*)\*1/3(*число информационных бит – кодирование*) =2/3=0,67 бит/с/Гц.

Для того чтобы определить число голосовых абонентов *N4*, нужно прежде всего вычислить скорость передачи данных, достижимую при заданных параметрах.

Алгоритм расчета пропускной способности базовой станции LTE:

а) Рассчитайте символьную скорость (символ/сек). Формула расчета:

*Общее число символов= (Число OFDM-символов в одном RB) х (Число RB по частоте в зависимости от ширины полосы) х (число RB в 1 мс субкадре) х (Число субкадров в 1 с) х (Число потоков данных с MIMO)*

б) Отнимите от общего числа символов символы, являющиеся затратами частотно-временных ресурсов на управление (каналы управления, опорные сигналы, сигнальные данные RRC-протокола и пр.) и символы, затрачиваемые на повторные передачи транспортных блоков HARQ.

в) Домножьте полученное число символов на спектральную эффективность одного символа, зная MCS, вы получите пропускную способность *C* в бит/с.

г) Разделив полученную скорость на скорость, требуемую для голосового соединения одного пользователя, получим число голосовых абонентов в сети LTE:

Пример исходных данных для расчета абонентской емкости сетей 4G:

* Ширина полосы частот: 10 МГц;
* Циклический префикс: нормальный;
* Требуемая скорость передачи данных для одного голосового абонента на физическом уровне *c*: 20 кбит/с;
* Режим MIMO: 2x2, пространственное мультиплексирование (spacial multiplexing);
* Затраты частотно-временных ресурсов на каналы управления и вспомогательные сигналы: 30%;
* Процент ретрансмиссий MAC-уровня HARQ: 10%;
* Используемая схема модуляции и кодирования MCS: QAM16 4/5;
* Режим дуплексирования UL и DL: FDD

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

[1] Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2012. - 943с.

[2] Практикум по работе с анализатором протоколов WireShark. URL: https://networkguru.ru/wireshark

[3]     Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] : монография / Б. Скляр. - 2-е изд., испр. - М. : Издат.дом "Вильямс", 2004. - 1099с.

[4] Jesin, A. Packet Tracer Network Simulator, Packt Publishing, 2014. – 134 p.

[5] Столлингс, В. Беспроводные линии связи и сети [Текст] = Wireless Communications and Networking : пер. с англ. : монография / В. Столлингс. - Москва : Вильямс, 2003. - 638 с. : ил. - Библиогр.: с. 623-629 . - Предм. указ.: с. 634-638. - Словарь терминов: с. 615-622 . - ISBN 5-8459-0409-9 (12)

[6] Шахнович, И. Современные технологии беспроводной связи [Текст] : монография / И. Шахнович. - М. : Техносфера, 2004. - 166с. (9)

[7] Попов, В. И. Основы сотовой связи стандарта GSM [Текст] : монография / В. И. Попов. - М. : Эко-Трендз, 2005. - 292с.

[8] Сети UMTS. Архитектура, мобильность, сервисы [Текст] : монография / Х.Кааранен, А. Ахтиайнен, Л. Лаитинен и др.; пер. с англ. Н.Л. Бирюкова. - М. : Техносфера, 2007. - 458с. (7)

[9]    Тихвинский, В. О. Сети мобильной связи LTE: Технологии и архитектура [Текст] : монография / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. - М. : Эко-Трендз, 2010. - 283с.