А.М. ГОЛИКОВ

ТРАНСПОРТНЫЕ И МУЛЬТИСЕРВИСНЫЕ СИСТЕМЫ И СЕТИ СВЯЗИ

Учебное пособие

для специалитетета: 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации)

Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу

Второе издание дополненное и переработанное

Томск 2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
Томский государственный университет систем управления и радиоэлектроники

А.М. ГОЛИКОВ

ТРАНСПОРТНЫЕ И МУЛЬТИСЕРВИСНЫЕ СИСТЕМЫ И СЕТИ СВЯЗИ

Учебное пособие

для специалитетета: 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации)

Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу

Второе издание дополненное и переработанное

Томск 2017

Голиков А.М. Транспортные и мультисервисные системы и сети связи: Учебное пособие. для специалитетета: 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации). Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу. Второе издание дополненное и переработанное – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2017. – 373 с.

Учебное пособие содержит лекционный материал, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу по транспортным и мультисервисным системам и сетям связи по курсу «Транспортные и мультисервисные системы и сети связи» специальности 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации). Представлены описания аппаратно-программных комплексов и методики построения систем, а также компьютерное моделирование мультисервисных систем. Мало учебников для комьютерной реализации реализации современных телекоммуникационных систем. Актуальность пособия велика, так как в современных системах связи и телевидения, а также кабельных сетях применяются все более сложные виды модуляции и кодирования, обеспечивающие высокую помехоустойчивость.

Методология изучения курса состоит в закреплении теоретических знаний на примерах компьютерной реализации современных телекоммуникационных систем и индивидуальных заданий на самостоятельную работу.

СОДЕРЖАНИЕ

ЧАСТЬ 1. Транспортные системы и сети связи

1. ОБЩАЯ ХАРАКТЕРИСТИКА МУЛЬТИМЕДИЙНОГО ТРАФИКА

Знание характеристик трафика, создаваемого пользователями (абонентами), является непременным условием для грамотного проектирования сетей электросвязи. Значение трафика непосредственно определяет как капитальные затраты на оборудование сети, так и возможные доходы за счет его эксплуатации.

1.1. Классификация мультимедийного трафика

Мультимедийный трафик. Под мультимедийным трафиком понимается цифровой поток данных, который содержит различные виды сообщений, воспринимаемых органами чувств человека (обычно звуковая и/или видеоинформация). Мультимедийные потоки данных передаются по телекоммуникационным сетям с целью предоставления удаленных интерактивных услуг. Наиболее распространенными на сегодняшний день мультимедийными услугами, предоставляемыми пользователям сети, являются: видеотелефония, высокоскоростная передача мультимедийных данных, 1Р-телефония, цифровое телевизионное вещание, мобильная видеосвязь и цифровое видео по запросу.

В зависимости от типа предоставляемого сервиса выделяются две основные категории мультимедийного трафика.

1. Трафик реального времени, предоставляющий мультимедийные услуги для передачи информации между пользователями в реальном масштабе времени.

2. Трафик обычных данных, который образуется традиционными распределенными услугами современной телекоммуникационной сети, таких, как электронная почта, передача файлов, виртуальный терминал, удаленный доступ к базам данных и др.

В качестве примеров услуг, генерирующих трафик реального времени, можно привести следующие: 1Р-телефония, высококачественный звук, видеотелефония, видеоконференцсвязь, дистанционное (удаленное) медицинское обслуживание (диагностика, мониторинг, консультация), видеомониторинг, широковещательное видео, цифровое телевидение, вещание радио- и телевизионных программ.

1Р-телефония. Данный сервис осуществляет передачу голосового трафика (речи) между двумя абонентами сети, в которой, в качестве сетевого, используется протокол IP (Internet Protocol). Для организации сервиса «IP-телефония» могут быть использованы локальные, корпоративные, глобальные сети, а также сеть Интернет. С помощью специальных шлюзов, используемых в телефонной сети общего пользования, обеспечивается IP-телефонная связь между абонентами телефонных сетей и абонентами сетей передачи данных.

Высококачественный звук. Под «высококачественным звуком» понимается такой сервис, который осуществляет передачу и вещание высококачественного звука, например, музыки, концертных выступлений и т.д.

Видеотелефония. Данный сервис осуществляет передачу человеческой речи вместе с его изображением невысокого качества между двумя абонентами. Клиенты данного сервиса, через соответствующую коммутационную аппаратуру, могут слушать и видеть друг друга в режиме реального времени.

Видеоконференция. Данный сервис осуществляет передачу голосового и видеотрафика между группой абонентов, причем звуковые и видеосигналы передаются по сети независимо один от другого (по разным транспортным соединениям), их синхронизация на приеме обеспечивается соответствующим протоколом транспортного уровня.

Дистанционное медицинское обслуживание. Данный сервис обеспечивает проведение дистанционного медицинского обследования, диагностики и консультации больных. Трафик данного сервиса включает голосовые и видеоданные, результаты обследования, переданные в реальном масштабе времени, и др.

Видеомониторинг. Данный сервис осуществляет видеонаблюдение помещений, применяется для охраны территорий различного назначения, оперативной сигнализации о различных нештатных ситуациях, постоянного (в режиме реального времени) мониторинга в местах скопления людей.

Вещание радио и телевизионных программ. Данный сервис осуществляет вещание обычных радио- и телевизионных каналов по цифровой телекоммуникационной сети.

Цифровое телевидение. Данный сервис осуществляет вещание высококачественного цифрового телевидения (художественных фильмов, музыкальных видеоклипов, спортивных трансляцией) по запросу клиентов данного сервиса.

Основной тенденцией в развитии современных телекоммуникационных сетей является поддержка различных видов сервиса, в том числе мультимедийного. Требования различных типов мультимедийного трафика к сетевым ресурсам могут отличаться весьма существенно. Например, обычный трафик, как правило, не налагает особых ограничений на время его доставки до получателя. Все что требуется такому трафику, - это выделение ему минимальной пропускной способности.

Другим примером может быть трафик для проведения видеоконференций в реальном масштабе времени. Он требует не только значительной пропускной способности, но также и минимизации времени доставки видеокадров до получателя. Кроме того, качество проведения сеанса видеоконференции не будет удовлетворительным, если задержки пакетов информации имеют слишком нерегулярный характер. В данном случае к ресурсам сети

предъявляются жесткие требования по многим параметрам. Эти параметры подробно будут рассмотрены ниже.

Описание и анализ мультимедийного трафика в современных телекоммуникационных сетях является сложной и трудной задачей. Основными причинами этих трудностей являются:

- широкий диапазон скоростей передачи - от нескольких кбит/с, как в случае передачи телефонного трафика, до сотен Мбит/с, при передаче видепотоков;

- разнообразные статистические свойства передаваемых мультимедийных информационных потоков (трафик реального времени налагает жесткие требовании к ресурсам сети);

- большое разнообразие сетевых конфигураций, множество технологий и протоколов передачи (Gigabit Ethernet, ATM, MPLS и др.);

- многоуровневая обработка передаваемых сообщений, вследствие чего качество обслуживания оказывается зависящим от нескольких уровней обработки.

1.2. Общий подход к параметризации мультимедийного трафика

Имеется множество моделей описания трафика в различных телекоммуникационных сетях.

В общем случае мультимедийный трафик некоторой услуги представляется в виде случайного процесса. Пусть мгновенное значение трафика - есть число блоков информации, которые генерирует соответствующий сервис в единицу времени. Тогда в наиболее общем случае случайный процесс $B(t)$ описывается семейством функции распределения $F_{B(t)}(x)$, где

$$F_{B(t)}(x)=Вер\{B(t)\ Ф\ x\}$$

Практическое использование такого метода описания затруднительно [не создан математический аппарат, обеспечивающий оценку параметров качества такой нестационарной нагрузки общего вида, сложность в адекватном оценивании семейства функции распределения $F_{B(t)}(x)$].

Для параметризации мультимедийного трафика, как правило, используется ряд характеристик, которые определены рекомендациями ITU-T. Эти характеристики описывают интегральные параметры случайного процесса $B(t)$, пример реализации которого приведен на рис. 1.1.

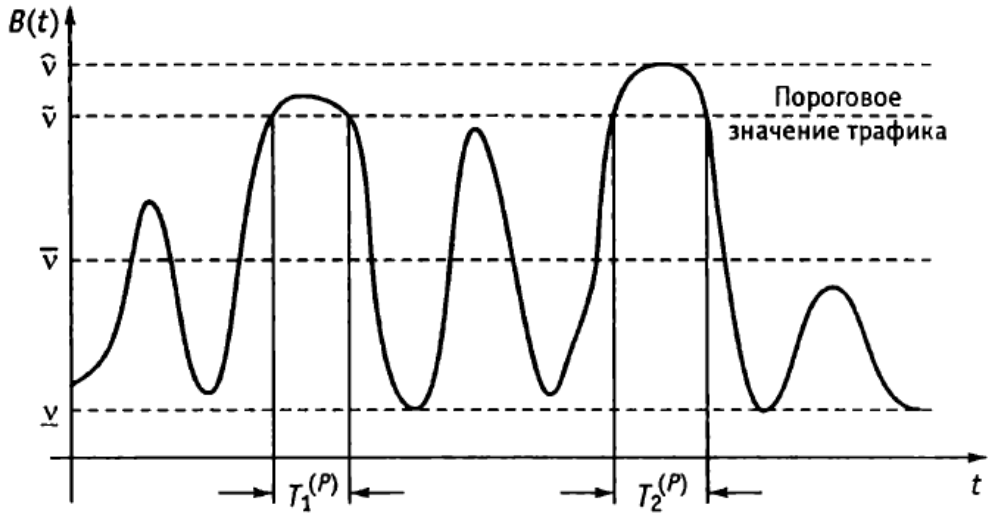


Рис. 1.1. - Основные параметры мультимедийного трафика

К характеристикам трафика, который генерируется различными мультимедийными услугами, относятся следующие:

- значения трафика (мгновенное, максимальное, пиковое, среднее и минимальное), бит/с;
- коэффициент пачечности трафика (пульсация);
- средняя длительность пикового трафика;
- средняя длительность сеанса связи;
- форматы элементов трафика;
- максимальный, средний, минимальный размеры пакета;
- интенсивность трафика запросов.

Максимальное значение трафика $\hat{v}$. Максимальное число блоков информации, которое соответствующий сервис генерирует в единицу времени, определяется как:

$$\hat{v} = maxB(t)$$

Пиковое значение трафика. Трафик соответствующего сервиса, который превышает установленный для него пиковый порог $\tilde{v}$.

Среднее значение трафика $\bar{v}$. Среднее число блоков информа ции, которое соответствующий сервис генерирует в единицу времени, определяется как

$$\bar{v} = \frac{1}{T^{(s)}} \int_0^{T^{(s)}} B(t)dt$$

где $T^{(s)}$ – длительность сеанса связи.

Минимальное значение трафика $\underline{v}$. Минимальное число блоков информации, которое соответствующий сервис генерирует в единицу времени, определяется как

$$\underline{v} = \min_t B(t)$$

Коэффициент пачечности трафика К. Определяется как отношение между максимальным и средним трафиком соответствующего сервиса. Коэффициент пачечности вычисляется по формуле:

$$K = \frac{\hat{v}}{\bar{v}}$$

Средняя длительность пика $\bar{T}^{(p)}$. Средняя длительность интервала времени, в течение которого, соответствующий сервис генерирует пиковый трафик, вычисляется по формуле:

$$\bar{T}^{(p)} = \frac{1}{N^{(p)}} \sum_{i=1}^{N^{(p)}} T_i^{(p)}$$

где $N^{(p)}$ – число пиков в течение сеанса связи; $T_i^{(p)}$ - длительность *i*-пика процесса *B(t)*, $i = \overline{1, N^{(p)}}$, а длительность *i*-пика определяется выражением

$$T_i^{(p)} = t_i^{(e)} - t_i^{(s)}$$

где $t_i^{(e)}$, $t_i^{(s)}$ - моменты начала и окончания i-пика, которые определяются следующими выражениями:

$$t_i^{(s)} = \min_{\substack{B(t)>\bar{v} \\ t>t_{i-1}^{(s)}}} t, \quad t_i^{(e)} = \min_{\substack{B(t)>\bar{v} \\ t>t_i^{(s)}}} t, \quad \text{где } t_0^{(s)}, t_0^{(e)} = 0.$$

Перечисленные выше параметры используются для описания трафика соответствующего сервиса в течение одного сеанса связи с абонентом сервиса.

Интенсивность запросов λ на получение обслуживания абонентами сети у соответствующего сервиса определяется как среднее число поступивших запросов на обслуживание в единицу времени.

Средняя длительность сеанса связи $\bar{T}^s$ – средняя продолжительность интервала времени, в течение которого соответствующий сервис обслуживает поступивший запрос.

Максимальный размер пакета $\hat{s}$ – максимальный размер элемента трафика в битах (элемент трафика передается адресату как единое целое).

Таблица 1.1. Параметры трафика мультимедийных услуг (типичные значения)

Тип ультимедийного сервиса	Параметры мультимедийных трафиков					
	$\hat{v}$, Мбит/с	$\bar{v}$, Мбит/с	K	$T_i^{(p)}$, с	$T_i^{(s)}$, с	λ, Сеанс/сут
IP-телефония	0,064	0,064	1	100	100	5
Высококачественный звук	1	1	1	53	53	3
Видеотелефония	10	2	5	1	100	6
Видеоконференция	10	2	5	1	1000	6

Дистанционное медицинское обслуживание	10	2	5	1	1000	3
Видеомониторинг	10	2	5	-	-	6
Вещание радио и телевизионных программ	34	34	1	-	-	6
Цифровое телевидение	34	34	1	-	5400	6

Средний размер пакета $\bar{s}$ – средний размер элемента трафика в битах.

Минимальный размер пакета $\underline{s}$- минимальный размер элемента трафика в битах.

Некоторые типичные параметры трафика, генерируемого соответствующими источниками, приведены в табл. 1.1.

1.3. Параметры качества обслуживания мультимедийного трафика в сетях

При передаче разного вида трафика, каждому пользователю должно быть представлено телекоммуникационное (транспортное) соединение, которое обеспечивает соответствующее этому трафику качество обслуживания в соответствии с международными рекомендациями и стандартами.

Выделяются следующие основные параметры качества соединения: 1) время установления соединения; 2) вероятность установления соединения; 3) вероятность разрыва соединения; 4) задержка; 5) вероятность потери; 6) джиттер.

Время установления соединения $t^{(cn)}$ – определяется как интервал времени от момента выдачи абонентом запроса на предоставление соответствующего мультимедийного сервиса до момента начала предоставления этого сервиса.

Вероятность установления соединения $P^{(cn)}$ – отношение числа запросов, которым уже предоставлен соответствующий сервис, к общему числу запросов на предоставление этого сервиса.

Вероятность разрыва соединения $P^{(rj)}$ – определяется как отношение числа запросов, которым соответствующий сервис не был предоставлен полностью, к общему числу обслуженных запросов.

Задержки τ_i – определяется как интервал времени между моментом начала передачи отправителям i-блока данных трафика соответствующего сервиса и моментом окончания приема этого же блока его получателем. Задержка τ_i, складывается из времен пакетизации, передачи и распространения передаваемых блоков данных по каналам связи между узлами телекоммуникационной сети, а также из времени ожидания этих блоков в очередях промежуточных коммутаторов и маршрутизаторов сети.

В асинхронной телекоммуникационной сети задержка блоков данных может быть различной для каждого блока и представляет собой случайную величину, которая выражается следующим образом:

$$\tau_i = \tau_i^p + \sum_{k=1}^{M} \tau_{ik}^{pr} + \sum_{j=1}^{N} \left(\tau_{ij}^{sr} + \tau_{ij}^{wt} \right),$$

где τ_i^p – случайная величина времени пакетизации *i*-блока данных трафика; M – общее число каналов связи между двумя абонентами сервиса; N – общее число коммутационных устройств, расположенных между двумя абонентами сервиса; τ_{ik}^{pr} – случайная величина времени распространения *i*-блока данных трафика по k-каналу связи; τ_{ij}^{sr} – случайная величина времени обслуживания *i*-блока данных трафика в *j*-коммутационном устройстве; τ_{ij}^{wt} – случайная величина времени ожидания в очереди *i*-блока данных трафика в j-коммутационном устройстве.

Средняя задержка $\bar{\tau}$ определяется как среднее значение всех задержек передаваемых блоков данных,

$$\bar{\tau} = \frac{1}{N^{(b)}} \sum_{i}^{N^{(b)}} \tau_i ,$$

где $N^{(b)}$ – общее число доставленных блоков данных.

Вероятность потери $P^{(rs)}$ определяется отношением числа не доставленных адресату блоков данных к общему числу переданных.

Джиттер $\sigma^{(\tau)}$ – определяется как разница между $\tau^{(max)}$ и $\tau^{(min)}$ задержкой передачи блоков данных трафика соответствующего сервиса

$$\sigma^{(\tau)} = \tau^{(max)} - \tau^{(min)},$$

где

$$\tau^{(min)} = \bar{\tau} - \sqrt{D[\bar{\tau}]}, \quad \tau^{(max)} = \bar{\tau} + \sqrt{D[\bar{\tau}]},$$

а дисперсия

$$D[\tau] = \frac{1}{N^{(b)}} \sum_{i=1}^{N^{(b)}} \left(\tau_i - \bar{\tau} \right)^2 .$$

Влияние параметров транспортного соединения на качество представляемого абонентам сервиса представлено в табл. 1.2.

Значения времени доставки и джиттера доставки являются важными сетевыми характеристиками для услуг, осуществляемых в реальном масштабе времени.

Допустимые значения задержки, джиттера, вероятности потери пакета, вероятности установления соединения, времени установления соединения и вероятности разрыва соединения, определенные для основных типов мультимедийных услуг, полученные в

результате исследований Европейского исследовательского центра в области телекоммуникаций (RACE - Research on Advanced Communication in Europe), приводятся в табл. 1.3.

Таблица 1.2. Влияние параметров транспортного соединения на качество предоставления сервиса

Параметры качества	Тип сервиса			
	телефонный	видеоконференции	видео по запросу	передача данных
Задержка	Значительное	Значительное	Умеренное	незначительное
Время установления соединения	Значительное	Значительное	Умеренное	Умеренное
Джиттер	Значительное	Значительное	Значительное	Незначительное
Вероятность потери	Умеренное	Умеренное	Умеренное	Значительное
Вероятность установления соединения	Значительное	Значительное	Значительное	Значительное
Вероятность разрыва соединения	Значительное	Значительное	Значительное	Незначительное

Примечание. Термины значительное, умеренное, незначительное означают: значительное - сильное влияние параметра телекоммуникационного соединения на качество предоставления сервиса. Большое значение этого параметра неприемлемо; умеренное - среднее влияние параметра телекоммуникационного соединения на качество предоставления сервиса. Небольшое значение этого параметра допустимо; незначительное - слабое влияние параметра телекоммуникационного соединения на качество предоставления сервиса. Большое значение этого параметра допустимо.

Таблица 1.3. Допустимые значения параметров качества обслуживания при передаче мультимедийного трафика

Тип сервиса	Параметры качества обслуживания				
	$t^{(cn)}$, с	$P^{(fl)}$	τ, мс	$P^{(ls)}$	σ_τ, с
IP-телефония	0,5…1	10^{-3}	25…500	10^{-3}	100…150
Видеоконференция	0,5…1	10^{-3}	30	10^{-3}	30…100
Цифровое видео по запросу	0,5…1	10^{-3}	30	10^{-3}	30…100
Передача обычных данных	0,5…1	10^{-6}	50…1000	10^{-6}	–
Телевизионное вещание	0,5…1	10^{-8}	1000	10^{-8}	–

1.4. Характеристика трафика в сетях связи Российской Федерации. Прогнозирование трафика.

Потребности абонентов (пользователей) в обмене информацией в настоящее время удовлетворяются тремя доступными средствами - стационарной сетью, сотовой сетью подвижной (мобильной) связи, Интернет.

Таблица 1.4. Прогноз трафика для РФ

Трафик/год	2002	2007	2015
ТфОП	22,9	29,5	40,7
Сотовые сети	1,1	4,9	11,0
Интернет	1,0	6,2	120

Среднее значение удельного абонентского трафика для стационарной сети ТфОП составляет 0,1 Эрл. Распределение абонентского трафика в час наибольшей нагрузки (ЧНН) подчиняется нормальному закону.

Удельный абонентский трафик для сотовой сети подвижной связи по результатам измерений составляет 0,009 Эрл, а плотность распределения трафика подчиняется нормальному закону.

Удельный абонентский трафик пользователей Интернет составляет около 0,1 Эрл. Распределение абонентского трафика подчиняется логарифмически нормальному закону со среднеквадратичным отклонением $\sigma = 0{,}45$ Эрл.

Входящий и исходящий трафики для абонентов ТфОП и сетей подвижной связи считаются равными. Вместе с тем для пользователей Интернет практически весь трафик может быть отнесен к входящему. Для трехмерного вектора входящего трафика пользователя в мультисервисных сетях $Y_0 = \{Y_ф, Y_с, Y_и\}$ ($Y_ф$, $Y_с$, $Y_и$, соответственно, трафик ТфОП, сотовой сети подвижной связи, Интернет) имеют место следующие количественные характеристики нагрузки:

$$Y_Ф = 0{,}05 \text{ Эрл}, \quad \sigma(Y_Ф) = 0{,}225 \text{ Эрл};$$
$$Y_С = 0{,}0045 \text{ Эрл}, \quad \sigma(Y_С) = 0{,}067 \text{ Эрл};$$
$$Y_И = 0{,}1 \text{ Эрл}, \quad \sigma(Y_И) = 0{,}45 \text{ Эрл}.$$

С точки зрения оператора сети связи, наиболее интересными являются значения трафика за определенный период времени и на перспективу. Эти значения для сетей связи Российской Федерации в миллиардах минуто-занятий в месяц приведены в табл. 1.4.

Быстрыми темпами растет трафик сотовых сетей. Число сотовых телефонов уже сравнялось с числом стационарных. В соответствии с прогнозами, предельное число сотовых телефонов в Российской Федерации с учетом существующего народонаселения в 144,8 млн. или в форме телефонной плотности 122,4%. В то же время предельное значение телефонной плотности в условиях ускоренного роста сотовой связи составит около 40%. Сегодня и на

ближайшую перспективу основная доля доходов операторов связи будет приходиться на голосовые услуги. Однако, учитывая бурный рост трафика передачи данных, операторы связи должны уже сейчас проектировать сети как мультисервисные.

Таблица 1.5. Распределение трафика по видам услуг

Категории услуг	Общий суточный трафик для крупных городов, Тбит	Общий трафик в ЧНН
Мультимедийные сообщения (MMS)	9,92	1,02
Голосовые услуги с расширенными возможностями (Rich Voice)	28,66	4,73
Информационные услуги	42,04	2,95
Мобильный Интернет	18,87	1,13
Мобильный доступ к локальным сетям Intranet/Extranet	78,14	6,70
Услуги определения местоположения (Location-Based Services)	1,30	0,09
Голосовые услуги	71,28	4,26
Всего:	249,21	20,88

Рассмотрим более подробно тенденции изменения трафика в сетях подвижной связи третьего поколения (UMTS), которые с полным основанием можно отнести к мультисервисным. В качестве примера возьмем страны Западной Европы и основные характеристики трафика, прогнозируемого на период до 2012 г.

В проведенных UMTS-Forum исследованиях трафика в сетях UMTS была использована модель, учитывающая:

– профили зон обслуживания (ячейка, город, страна, регион, в мировом масштабе);
– профили абонентов (демографические данные - возраст, денежный доход, область деятельности и род занятий);
– сегмент рынка услуг (корпоративные клиенты, массовый рынок);
– тип соединения (машина-машина, человек-человек, человек-машина, точка-точка, точка-много точек);
– тип мультимедийного трафика (с высокой и низкой скоростями передачи данных);
– качество услуг (по таким параметрам, как время задержки пакетов, скорость передачи данных, приоритет предоставления услуги);
– тип терминального оборудования (ноутбук, карманный компьютер, мобильный телефон) и др.

Исследование строилось на анализе ранее полученных данных о состоянии рынка (Previous Analysis from Market Study) и текущем его изучении и прогнозировании (Current Study).

Данные исследований, приведенные в табл. 1.5, характеризуют распределение общего трафика (Тбит = 10^{12} бит) в крупных городах по видам услуг. Большая его доля приходится

на мобильный доступ к Интернет и локальным сетям, обычные голосовые услуги и информационные услуги. Однако приведенные в таблице услуги имеют характерное отличие по трафику в час наибольшей нагрузки (ЧНН). Так, наиболее выраженный пиковый характер трафика принадлежит мобильному доступу к Интернет (доступу к сетям Intranet/Extranet), обычным голосовым услугам и голосовым услугам с расширенными возможностями (Rich Voice). Суточное распределение трафика для некоторых услуг передачи данных показано на рис. 1.2-1.5.

Рассмотрим более подробно данные исследований по характеристике трафика для отдельных видов услуг передачи данных.

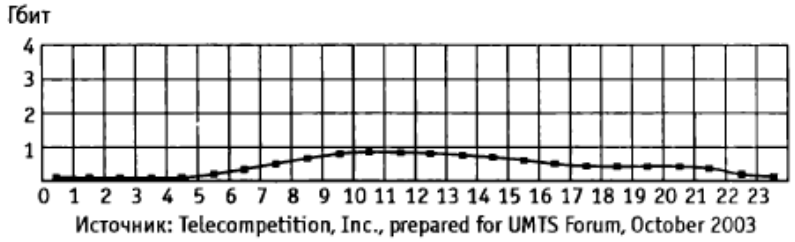


Рис. 1.2. Суточное распределение трафика MMS

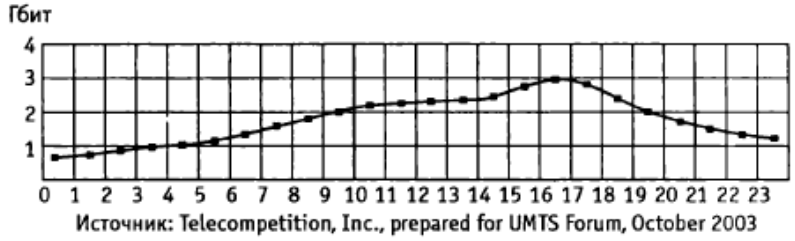


Рис. 1.3. Суточное распределение трафика информационных услуг

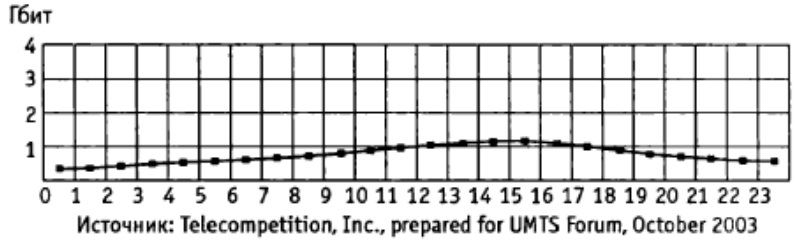


Рис. 1.4. Суточное распределение трафика мобильного Интернета

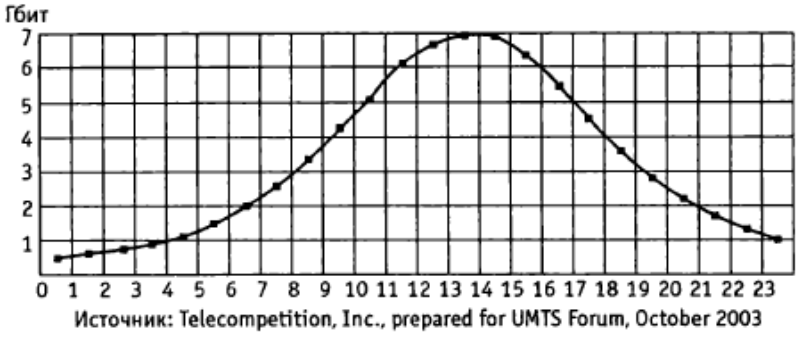


Рис. 1.5. Суточное распределение трафика мобильного доступа к Intranet/Extranet

Мобильный доступ к Интернет. Исследованы услуги для взрослых пользователей:

– электронная почта;

– «скачивание» видео- и аудио-файлов;

– мобильная торговля в Интернет;

для молодежи:

– электронная почта;

– «скачивание» мультимедийных файлов;

– мобильные игры.

В табл. 1.6 приведены данные о средних размерах файлов, передаваемых от пользователя и к пользователю при мобильном доступе в Интернет, а также асимметрии трафика в этих направлениях.

Услуги на основе определения местоположения абонента (LBS). Исследованы пять видов услуг LBS:

– информационные услуги по месту нахождения абонента (реклама, путеводитель);

– бизнес-приложения;

– навигация для автомобилистов;

– слежение за передвижением грузов;

– слежение за детьми, пожилыми людьми, животными.

Данные о средних размерах файлов, передаваемых от пользователя (UP) и (DL) к пользователю, приведены в табл. 1.7.

Услуги мультимедиа (MMS). Исследованы следующие виды услуг MMS:

Таблица 1.6. **Размеры файлов и асимметрия трафика**

Категория услуг	Линия «вверх» (UL), кбит	Линия «вниз» (DL), кбит	Асимметрия трафика (UL:DL)
E-mail	436	1746	1:4
Скачивание видео/ аудио	189	4725	1:25
Web Browsing	454	3175	1:7
MMS	189	4725	1:25
Мобильные игры	288	7200	1:25

Таблица 1.7. **Средние размеры файлов, передаваемых от пользователя к пользователю**

Категория услуг	Линия «вверх» (UL), кбит	Линия «вниз» (DL), кбит	Асимметрия трафика (UL:DL)
Реклама по месту абонента	0	100	0:1
Навигация (путеводитель)	83	100	1:1,2
Персональное отслеживание	0,01	0,02	1:1
Слежение за передвижением грузов	0,01	0,01	1:1
Телематические услуги	83	166	1:2

Таблица 1.8. **Средние размеры файлов при передаче MMS**

Типы терминалов	Категории сообщений	Длина сообщения, кбит
Обычные терминалы	Текст и графика с низким разрешением	10
	Фото	30
	Видео	100
Сложные терминалы	Текст и графика с низким разрешением	30
	Фото	100
	Видео	150

человек-человек:

– передача коротких видеоклипов;

– передача фото;

– передача текста с графическими вставками с невысоким разрешением;

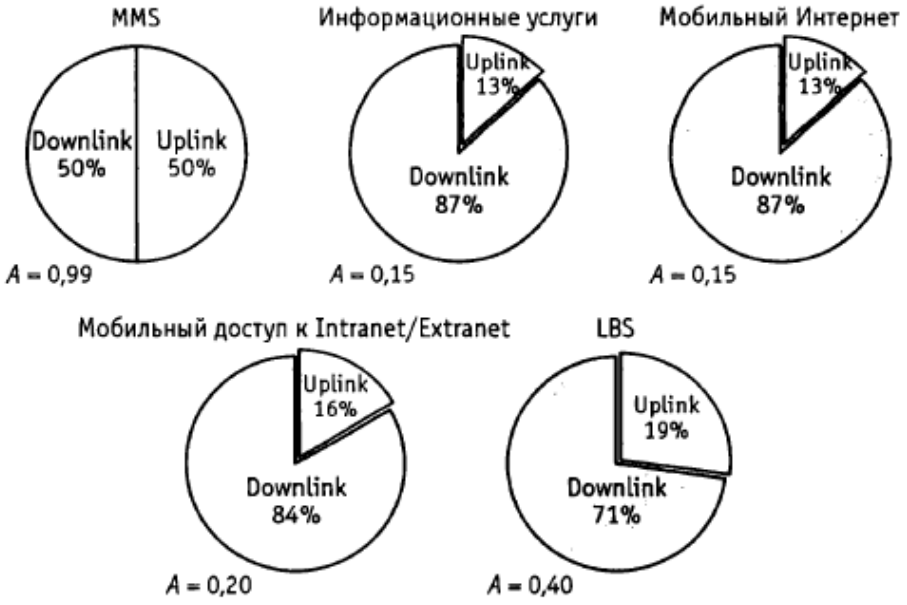
машина-машина (телематические услуги):

– просмотр объектов;

– передача информационно-развлекательных программ (к примеру, между различными серверами).

Данные о средних размерах файлов при передаче ММБ для различных типов терминалов приведены в табл. 1.8.

Часы набольшей нагрузки (трафика ММЭ) для корпоративных пользователей и массового рынка имеют ярко выраженное отличие: для корпоративных пользователей - это дневное время (10.00–13.00), для массового рынка - 19.00-21.00. При этом доля корпоративных ММ8-клиентов составляет 19%, доля массового рынка ММЭ – 12% от общего числа пользователей услугами 3в. Число передаваемых ими ММ8-сообщений в день составляет 5 и 11 соответственно. По типам ММЭ-сообщения распределяются следующим образом: 66% – текстовые сообщения с элементами графики невысокого разрешения, 24% – фото, 10% – сообщения с видеокомпонентами. По взаимодействию сетей: 32% – мобильная-мобильная, 40% - мобильная фиксированная, 28% – фиксированная-мобильная.



Источник: Telecompetition, Inc., prepared for UMTS Forum, October 2003

Рис. 1.6. Асимметричность трафика для различных видов услуг

Практически для всех видов услуг в сетях UMTS трафик имеет яр ко выраженный характер асимметричности. На рис. 1.6 показана асимметрия (A) трафика для различных услуг в каналах UP и DL в час наибольшей нагрузки.

Приведенные характеристики трафика в сетях UMTS позволяют сформировать представление о развитии рынка услуг 3G в Европе и в то же время ярко свидетельствуют о сложном его характере, который необходимо учитывать при проектировании и планировании сетей UMTS в России.

2. ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ПОСТРОЕНИЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ

На сетях связи межрегиональных компаний (МРК) сегодня используются различные технологии. Как видно из материалов ЛОНИИС, представленных в табл. 3.1, большинство операторов избрали подход, ориентированный на использование в качестве базовой технологии группы технологий IP-MPLS-ATM. Для переноса IP-трафика большинство операторов склоняются к двум вариантам IP over SDH и MPOA (Multiprotocol over ATM).

Таблица 3.1. **Технологии на сетях МРК**

Межрегиональная компания	Базовая технология мультисервисной сети	Метод переноса IP-трафика		
		IP over SDH	MPOA	MPLS
ОАО «МГТС»	IP-MPLS-ATM	–	–	+
Центральный регион	ATM	+	–	+
Северо-Западный регион	IP-MPLS-ATM	+	+	–
Приволжский регион	IP-MPLS-ATM	+	+	–
Южный регион	ATM	+	+	–
Уральский регион	IP-MPLS-ATM	+	+	–
Сибирский регион	ATM	+	–	–
Дальневосточный регион	ATM	+	+	–

2.1. Физический уровень. Волновое уплотнение (WDM, DWDM, CWDM)

В настоящее время на сетях России используются преимущественно оптические волокна, соответствующие рекомендации G.652 и синхронные мультиплексоры уровня STM-16 (2,5 Гбит/с) без оптических усилителей с длиной участка регенерации до 100... 120 км. В то же время, волоконно-оптические линии обладают существенно более высокой пропускной способностью.

Действительно, теоретический предел пропускной способности оптического волокна (ОВ) в третьем окне прозрачности, т.е. на частоте порядка 193 ГГц, составляет примерно 3-109 ОЦК. В то же время для STM-16 число ОЦК 3-105, что составляет 0,01% от пропускной способности ОВ. Повысить коэффициент использования оптического волокна и, следовательно, решить проблему нехватки оптического волокна, можно за счет волнового уплотнения (Wave length-Division Multiplexing, WDM). В литературе, применительно к WDM, также встречается термин «спектральное мультиплексирование по волнам» и «волновое мультиплексирование».

В зависимости от числа волн, размещаемых в одном ОВ, различают технологии WWDM, CWDM, DWDM и HWDM. Так, если в ОВ организовано всего два канала с использованием окон прозрачности 1300 и 1500 нм, то это технология с разнесенным спектральным мультиплексированием (Wide Band Wave Length Division Multiplexing, WWDM).

Системы грубого волнового мультиплексирования (Coarse WDM) работают в спектральном диапазоне 1300... 1650 нм, используя 16 оптических несущих, интервалы между которыми 20 нм. В DWDM используется до 160 оптических несущих с выделением для каждого из каналов полосы 25...50 ГГц.

Главное достоинство технологий WDM заключается в том, что они позволяют преодолеть ограничения на пропускную способность канала и существенно увеличить скорость передачи данных. Причем используются уже проложенный волоконно-оптический кабель и стандартная аппаратура временного мультиплексирования. Благодаря WDM удается организовать двустороннюю многоканальную передачу трафика по одному волокну (в обычных линиях используется пара волокон - для передачи в прямом и обратном направлениях).

Существенно и то, что в сетях SDH появилась возможность выбирать для отдельного канала значение скорости (уровень иерархии), не зависящее от скорости других каналов, и затем использовать разные методы передачи. Наконец, распространению WDM способствуют последние технологические достижения: создание узкополосных полупроводниковых лазеров, имеющих ширину спектра излучения менее 0,1 нм, широкополосных оптических усилителей и оптических фильтров для разделения близких каналов.

Может сложиться представление, что технологии WDM являются универсальным решением проблемы увеличения пропускной способности, некой панацеей от всех бед, с которыми сталкиваются пользователи глобальных сетей. Между тем применение WDM тормозится рядом факторов как экономического, так и чисто технического характера.

Если говорить об экономической стороне дела, то внедрение WDM в местных сетях сдерживается высокой стоимостью соответствующей аппаратуры, особенно передающих устройств, и сложностью коммутации трафика. Вместе с тем исследования показывают, что решения на базе WDM могут оказаться экономически эффективными и в сетях меньшего масштаба. Для этого, в частности, в них должны применяться недорогие мультиплексоры ввода/вывода, устанавливаемые в местах сопряжения местных и опорных сетей.

Фактор высокой стоимости аппаратуры оказывается еще более существенным для реализации технологии DWDM. При использовании близких частот требуются узкополосные полупроводниковые лазеры с высокой стабильностью длины волны генерируемого излучения, которые являются наиболее дорогим элементом DWDM-систем, сдерживающим распространение последних. Тем не менее основными преимуществами технологий DWDM остаются:

- высокие скорости передачи, и как следствие, высокий коэффициент использования ОВ;

- возможность обеспечения 100%-ной защиты на основе кольцевой топологии и простого наращивания каналов в оптической магистрали.

В настоящее время сети DWDM применяются для построения высокоскоростных транспортных сетей операторов национального масштаба, на основе топологий «точка-точка» или «кольцо» и мощных городских транспортных магистралей, которые могут использоваться большим количеством пользователей с потребностями в высоких скоростях передачи и использующих различные протоколы.

Специалисты по организации оптических сетей связи отмечают, что при использовании WDM отсутствуют многие ограничения и технологические трудности, свойственные TDM. Для лучшего использования пропускной способности ОВ вместо увеличения скорости передачи в едином составном канале, как это реализовано в TDM, в технологии WDM увеличивают число каналов (длин волн), применяемых в системах передачи.

Повышение скорости передачи при использовании технологии WDM осуществляется без дорогостоящей замены оптического кабеля. Применение технологий WDM позволяет сдавать в аренду не только оптические кабели или волокна, но и отдельные длины волн, т.е. реализовать концепцию «виртуального волокна». По одному волокну на разных длинах волн можно одновременно передавать самые разные приложения - кабельное телевидение, телефонию, трафик Интернета, «видео по требованию» и т.д. Как следствие, часть волокон в оптическом кабеле можно использовать для резерва.

Применение технологий WDM позволяет исключить дополнительную прокладку оптических кабелей в существующей сети. Даже если в будущем стоимость волокна уменьшится за счет использования новых технологий, волоконно-оптическая инфраструктура (проложенное волокно и установленное оборудование) всегда будет стоить достаточно дорого. Для ее эффективного использования необходимо иметь возможность в течение долгого времени увеличивать пропускную способность сети и менять набор предоставляемых услуг без замены оптического кабеля. Технологии WDM предоставляют такую возможность.

Технологии WDM используются пока в основном на линиях связи большой протяженности, где требуется большая полоса пропускания. Сети городского и регионального масштаба и системы кабельного телевидения потенциально также являются широким рынком для технологий WDM.

В то же время применение технологий DWDM предъявляет существенно более высокие требования к оборудованию и компонентам линии и, соответственно, к точности расчета их параметров. Чтобы возможности ВОЛС соответствовали запросам рынка, важно правильно

спланировать их развитие. Это позволит распределить затраты на строительство ВОЛС во времени и наращивать их емкость с учетом запросов потребителей.

2.2. Технологии канального, сетевого и транспортного уровней

2.2.1. Технология IP-сетей

Структура стека протоколов TCP/IP. Архитектура протоколов Интернета четырехуровневая. Появившуюся намного позже семиуровневую архитектуру протоколов эталонной модели ISO можно рассматривать как дальнейшее развитие TCP/IP - декомпозицию двух уровней TCP/IP. Действительно, отличие двух архитектур состоит в том, что три высших уровня (прикладной, представления данных, сеансовый) модели OSI в архитектуре TCP/IP объединены в один - прикладной (рис. 3.20). Уровень сетевых интерфейсов TCP/IP соответствует двум уровням OSI - канальному и сетевому.

Прикладной уровень TCP/IP поддерживает традиционные услуги:

– электронная почта и обмен новостями, которые реализуются с помощью простого протокола передачи электронной почты SMNP (Simple Mail Transfer Protocol); почтовых протоколов IMAP (Internet Message Access Protocol), POP (Post Office Protocol) и X.400; сетевого протокола обмена новостями NNTP (Network News Transfer Protocol);

– виртуальный терминал реализуется с помощью протокола Telnet;

– передача файлов осуществляется с помощью протоколов FTP (Fail Transfer Protocol), TFTP (Trivial File Transfer Protocol) и NFS (Network File Systems);

– справочные службы реализуются с помощью системы доменных имен DNS (Domain Name System) и X.500;

– вспомогательные протоколы: получения собственных идентификаторов – BOOTP, времени – NTP (Network Time Protocol), диагностики – Echo и информации о системе – Finger.

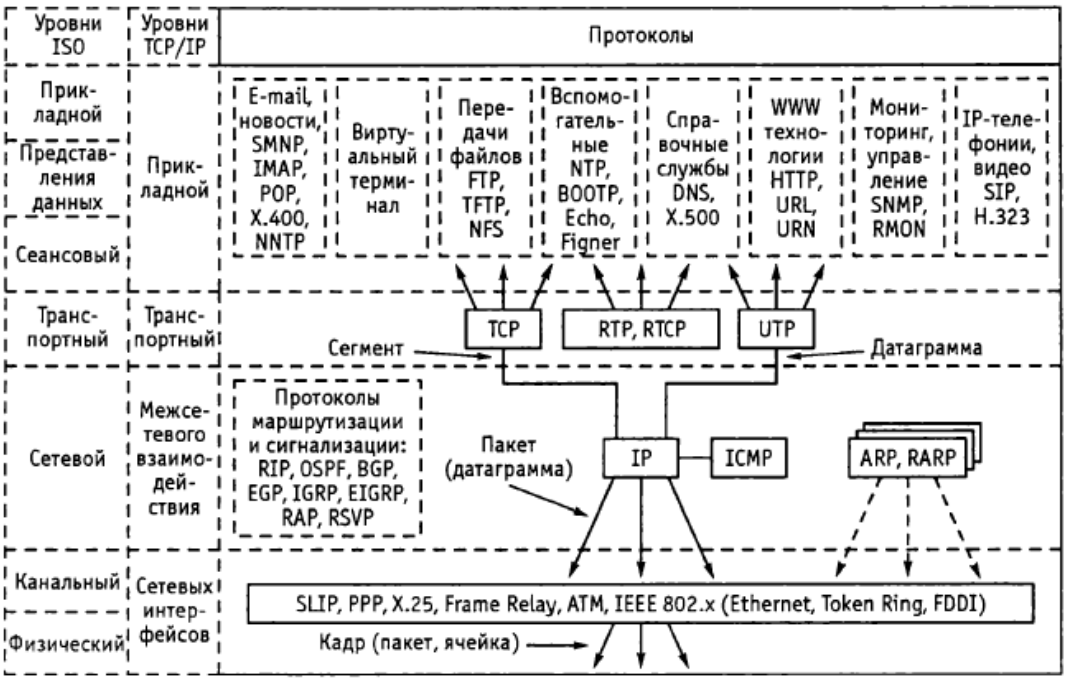


Рис. 3.20. Структура стека протоколов TCP/IP

В середине 1990-х годов активно внедрялись услуги, базирующиеся на технологии WWW (World Wide Web), основанной на протоколе передачи гипертекста (Hypertext Transfer Protocol, HTTP) с использованием URL (Universal Resource Locator) и URN (Universal Resource Names).

Сегодня популярны услуги пакетной IP-телефонии на базе протоколов SIP (Session Initiation Protocol), RTP (Real-time Transport Protocol), RTCP (Real-rime Transport Control Protocol), рекомендаций H.323 и др.

Особое место в стеке занимают протоколы мониторинга и управления:

– SNMP (Simple Network Management Protocol);

– RMON (Remote Monitoring).

С помощью этих протоколов отслеживают состояние сети и проводят ее администрирование.

Для сетевого взаимодействия большинство приложений пользуются услугами протоколов транспортного уровня TCP и UDP. Протокол TCP гарантирует надежную полнодуплексную передачу сегментов данных с предварительным установлением логического соединения.

Протокол датаграмм пользователя UDP (User Datagram Protocol) обеспечивает передачу датаграмм без установления соединения, что не гарантирует их доставку.

Передачу пакетов между сетями различной архитектуры обеспечивает основной протокол стека - IP. Датаграммный протокол IP не гарантирует надежной передачи пакетов, что, однако, увеличивает пропускную способность при передаче данных через множество сетей.

На сетевом уровне также используются:

– диагностический протокол ICMP (Internet Control Message Protocol), который передает сообщения узлам сети об ошибках и сбоях в передаче;

– протоколы разрешения проблемы адресов: ARP (Address Resolution Protocol) трансформирует IP адрес в физический адрес узла сети (MAC - адрес станции); RARP (Reverse Address Resolution Protocol) выполняет обратную функцию, т. е. с помощью MAC адреса определяет IP адрес.

Работу сетевого уровня поддерживают ряд протоколов маршрутизации и сигнализации: RIP (Routing Internet Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP), BGP (Border Gateway Protocol), RAP (Routing Access Protocol), RSVP (Resource Reservation Protocol) и др.

Стек протоколов TCP/IP взаимодействует на канальном уровне с большим количеством протоколов и сетевых технологий, которые инкапсулируют пакеты IP протокола. На сегодня вопросам взаимодействия Интернета с другими сетями посвящено более 290 документов RFC.

Чтобы выяснить, как выполняется передача данных с помощью любой технологии, необходимо рассмотреть следующее:

1) как формируется и распределяется адресное пространство сети;

2) логические характеристики (назначение полей пакетов) основных протоколов IP-технологии;

3) основные процедурные характеристики протоколов, которые обеспечивают нормальное функционирование процесса передачи информации;

4) каким образом решается вопрос определения путей передачи данных от отправителя к получателю, т. е. как маршрутизируются пакеты.

Опуская рассмотрение вопросов 1-3, перейдем к пункту 4.

Методы маршрутизации. Протоколы маршрутизации (см. рис. 3.20) представляют собой наиболее сложную группу протоколов Интернет, которая динамично развивается. Под маршрутизацией понимают решение задачи поиска оптимального пути от отправителя информации к ее получателю. Оборудование, которое решает эту задачу, называют маршрутизаторами (router). В IP-сетях (Интернет и др.) главным параметром маршрутизации является адрес в IP-протоколе. Сеть Интернет организована как совокупность взаимосвязанных между собою автономных систем или доменов (domains). Автономная система включает в себя IP-сети, которые имеют единое административное управление и общую политику (стратегию) маршрутизации (policy routing). В пределах домена используются протоколы внутренней (Interior Gateway Protocol, IGP), а между ними протоколы внешней маршрутизации (Exterior Gateway Protocol, EGP).

При рассмотрении маршрутизации выделяют две проблемы:

– определение и распространение сведений о маршрутах в сети (домене), которые связаны с реализацией политики маршрутизации и регламентируются алгоритмами «вектор-расстояние» (distance vector) и «состояния каналов» (link state);

– продвижение по установленным маршрутам пакетов от отправителя к получателю, которое определяется алгоритмами поэтапной маршрутизации (hop-by-hop routing) и маршрутизацией от источника (source specified routing).

Алгоритм «вектор-расстояние» базируется на том, что каждый объект (маршрутизатор), который принимает участие в маршрутизации, сохраняет в своей базе информацию обо всех адресах сети и метрику - расстояние до получателя информации. Объекты обмениваются между собой маршрутными базами. При принятии решения о маршруте передачи пакета оценивается каждый путь к объекту и выбирается наилучший. Этот алгоритм реализован в протоколах маршрутизации RIP и IGRP.

Алгоритм состояния каналов. Здесь на первом этапе каждый объект формирует топологическую базу (link state database) и строит граф связей сети, который описывает ее топологию с учетом того, что каждая связь (канал) характеризуется своей метрикой. Объекты, обмениваясь базами, обновляют сведения о сетях. На втором этапе объект решает проблему определения оптимального пути к каждой известной ему сети. Этот алгоритм реализован в протоколах OSPF и EIGRP.

Поэтапная маршрутизация. В этом методе каждый маршрутизатор принимает независимое решение о продвижении пакета на основании адреса получателя и информации, которая находится в маршрутной базе.

Маршрутизация от источника. Маршрут формируется отправителем пакета и записывается в каждый пакет, который отправляется в сеть.

Протокол RIP. Протокол RIP - это протокол внутренней маршрутизации, предназначенный для небольших доменов. Первая версия протокола RIP стандартизирована RFC 1058, а вторая - RFC 1722 и др. RIP для передачи сообщений использует протокол UDP (порт 520). Сообщения RIP состоят из IP-адреса сети и числа шагов (маршрутизаторов) к ней. Максимальное количество шагов - 15. В одном сообщении RIP может быть информация о 25 сетях. Маршрутизатор, на котором работает RIP, получая сообщения RIP от других маршрутизаторов, строит свою таблицу маршрутизации, в которой прописаны пути к другим сетям. Обмениваясь RIP сообщениями, маршрутизаторы каждые 30 секунд обновляют свои таблицы маршрутизации и с их помощью выполняют продвижение пакетов по сети.

Недостатки протокола:

– не всегда выбирается самый эффективный маршрут;

– из-за медленной сходимости образуются логические петли и медленно возобновляются таблицы после сбоя в работе маршрутизатора;

– используются широковещательные рассылки большого количества служебной информации (таблицы маршрутизации), которые загружают сеть;

– ограничен размер домена маршрутизации (15 переходов);

– не работает с адресами подсетей и не различает автономных систем.

Протокол OSPF стандартизирован в RFC 1370, 1578, 1793, 1850, 2328. Применяется для внутренней и внешней маршрутизации, используя алгоритм состояния каналов. Может обслуживать автономную систему, которая состоит из нескольких зон. Протокол OSPF значительно эффективнее протокола RIP. Маршрутизатор, на котором работает OSPF, решает проблему оптимизации маршрутов, анализируя граф сети с метрикой, характеризующей качество обслуживания.

Основными параметрами метрики являются: пропускная способность, задержка, надежность, а дополнительными - загрузка канала, безопасность. Маршрутизаторы обмениваются сообщениями только при изменении топологии сети. OSPF быстрее, чем RIP, перестраивает маршрутную таблицу.

К основным преимуществам OSPF относятся:

– применение групповой передачи коротких сообщений при изменении топологии сети, что снижает непроизводительную загрузку сети;

– поддержка распределения информации по параллельным каналам в зависимости от их пропускной способности, что улучшает работу сети в целом (более подробно OSPF дано в приложении).

Протоколы IGRP и EIGRP. Эти протоколы разработаны фирмой Cisco Systems и используются для внутренней маршрутизации. IGRP использует алгоритм «вектор-расстояние», имеет значительно лучшие характеристики, чем протокол RIP, в частности:

– надежно работает в сетях сложной топологии;

– обладает лучшей, чем RIP, сходимостью;

– значительно снижает объем передачи служебной информации;

– распределяет информацию между каналами с одинаковыми метриками.

В метрику протокола входят следующие параметры канала: пропускная способность, задержка, нагрузка, надежность. Эти параметры могут меняться в широких пределах. Например, пропускная способность может изменяться от 1200 бит/с до 10 Гбит/с.

EIGRP - это протокол, который объединяет все преимущества алгоритмов «вектор-расстояние» и «состояния каналов». Протокол реализован на базе алгоритма распределенного обновления - (Distributed Update Algorithm, DUAL), который позволяет

маршрутизатору быстро возобновлять работу после изменения сетевой топологии. Протокол имеет:

– возможность находить соседа;

– алгоритм DUAL;

– усовершенствованный механизм инкапсуляции сообщений в IP.

В первую очередь маршрутизатор определяет достижимость своего «соседа» – маршрутизатора, который напрямую взаимодействует с ним. Для этого он периодически посылает пакет Hello. Затем алгоритм DUAL по полученной от «соседей» информации о маршрутах определяет оптимальный маршрут передачи нагрузки, который не является частью петли маршрутизации.

Протоколы EGP и BGP принадлежат к протоколам внешней маршрутизации сети Интернет. С помощью EGP взаимодействуют выделенные маршрутизаторы разных автономных систем, которые собирают информацию о системе с помощью внутренних протоколов маршрутизации.

К недостаткам EGP можно отнести следующее: не используется метрика, т.е. не выполняется интеллектуальная маршрутизация; не отслеживается появление петель маршрутов; служебные сообщения имеют большой размер.

В последнее время вместо EGP используют более совершенный протокол BGP, который, в свою очередь, для передачи служебных сообщений использует протокол TCP. Это повышает надежность при взаимодействии между автономными системами, поскольку TCP гарантирует доставку маршрутной информации. BGP полностью исключает недостатки протокола EGP. В качестве метрики используется скорость передачи в канале, его надежность и т.п. На сегодня BGP (третья версия) - это основной протокол сети Интернет, который определяет маршруты к удаленным автономным системам.

2.2.2. Технология ATM

Технология ATM считается наиболее «мультисервисной». Она позволяет достаточно эффективно решать задачи объединения сетей, построенных с использованием различных технологий передачи данных, обеспечения необходимого качества обслуживания и др. Все операторы МРК используют эту технологию (см. табл. 3.1) и основная конкуренция при создании МСС ожидается между технологиями ATM и MPLS. Большинство специалистов предрекают победу MPLS.

Напомним, что в ATM используются пакеты небольшой длины фиксированного размера (53 байта), называемые ячейками, и очень простые функции в транзитных узлах. Обнаружение и исправление ошибок осуществляется только в заголовке. Для содержимого информационных ячеек никакой проверки и восстановления не применяется, и используется

передача информации, ориентированная на соединение. Реализация ATM обычно осуществляется аппаратным обеспечением. Все это в сочетании с статистическим мультиплексированием уменьшает время задержек, что особенно важно при передаче трафика реального времени.

Технология ATM предоставляет методы управления трафиком и механизмы качества обслуживания. Это означает, что в сетях ATM могут быть зарезервированы ресурсы, гарантирующие требуемые значения пропускной способности, задержки передачи и уровня потерь ячеек. Стек протоколов ATM. В стеке протоколов ATM (рис. 3.21) различают следующие уровни: адаптации, ATM и физический. Уровень адаптации ATM (ATM Adaptation layer, AAL) делится на два подуровня конвергенции (Convergence Sub-layer, CS) и сегментации и восстановления (Segmentation And Reassebly, SAR). Уровень адаптации ATM по сути является интерфейсом между приложениями пользователя и уровнем ATM и обеспечивает поддержку четырех различных групп (классов) приложений.

Рис. 3.21. Стек протоколов ATM

Все приложения используют один и тот же подуровень SAR, но каждый тип приложений реализует свой собственный специфический подуровень CS.

После краткого рассмотрения подуровней AAL перейдем к их более полному описанию.

Подуровень конвергенции (CS) отвечает за получение протокольного модуля данных (Protocol Data Unit, PDU) от вышележащих уровней и их адаптацию, обычно за счет добавления служебной информации для дальнейшего представления уровню SAR. Так как каждый тип трафика требует специфической обработки, различают четыре типа уровней адаптации AAL.

Задачей подуровня SAR является формирование модулей длиной 48 октетов, которые становятся полезной нагрузкой ячеек ATM. Правило функционирования подуровня SAR заключается в том, что ничто не покидает подуровень, если его длина не равняется 48 октетам. В некоторых случаях в подуровне SAR могут добавляться свои собственные данные к модулю PDU подуровня CS, в других - он просто «нарезает» модули PDU подуровня CS в модули по 48 октетов и передает их вниз на уровень ATM.

Уровень ATM соответствует нижней части канального уровня модели OSI. Его основной задачей является коммутация ячеек способом, подходящим для осуществления их передачи

между отправителем и получателем. Основным модулем на уровне ATM является ячейка. Как упоминалось выше, длина ячейки составляет 53 октета, из которых 48 предназначены для переноса полезной нагрузки, оставшиеся 5 октетов - для служебной информации уровня ATM, т. е. заголовка ячейки ATM.

Сети ATM на физическом уровне обычно используются SDH.

На рис. 3.22 представлена обобщенная структура операций, осуществляемых на различных уровнях ATM. Здесь H - означает заголовок (Head), T - концевик (Trailer).

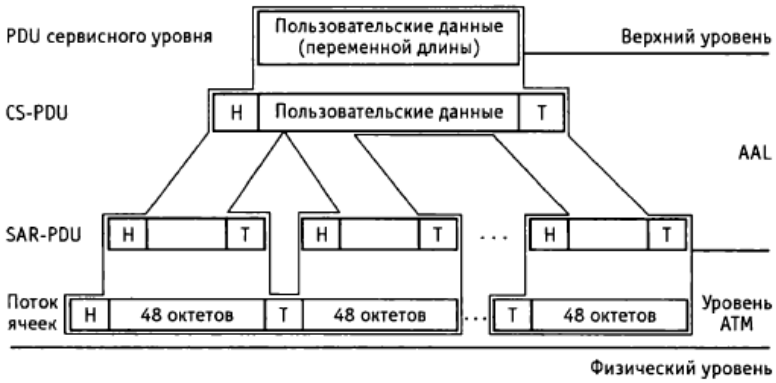


Рис. 3.22. Операции протокола ATM

Модуль PDU протокола вышележащего уровня (например, IP-пакет) поступает на подуровень CS уровня адаптации. Там путем добавления служебной информации к модулю PDU вышележащего уровня формируется модуль CS-PDU. Каждый тип AAL имеет свой специфический подход к формированию этой служебной информации. После того как модуль CS-PDU сформирован, он передается подуровню SAR. Основная задача подуровня SAR заключается в сегментации модуля CS-PDU на блоки длиной 48 октетов. На уровне ATM к ним добавляется 5 октетов заголовка ячейки. Затем ячейки преобразуются в формат соответствующего протокола физического уровня. На принимающей стороне процесс, показанный на рис. 3.22, происходит в обратном порядке.

Классы обслуживания AAL (рис. 3.23). Различают четыре класса обслуживания, охватывающие определенные типы трафика, которые, по мнению создателей ATM, встречаются в настоящее время или могут появиться в будущем. Услуга класса A является сервисом с установлением соединения. Он поддерживает трафик с постоянной скоростью битов, который требует сквозной синхронизации. Этот класс услуг обычно используется для передачи потоковых речевых и видеосигналов без сжатия.

Трафик (класс услуги)	Звук (A)	Видео со сжатием (B)	Данные, FR, … (C)	LAN (D)
Синхронизация	Требуется		Не требуется	
Скорость	Постоянная	Переменная	Переменная доступная	Переменная неопределенная
Соединение	Установление соединения, виртуальные каналы			Без соединения
Тип AAL	AAL1	AAL2	AAL3/4	
			AAL5	
Временной параметр	Реальное	Реальное/ нереальное	Нереальное	

Рис. 3.23. Классы обслуживания AAL

Услуга класса B является сервисом с установлением соединения и отличается от сервиса класса A только поддержкой сигналов с переменной скоростью передачи битов. Для трафика, который использует сервис класса B, также требуется синхронизация. Сигналы, которым необходима услуга класса B, включают сжатые и разбитые на пакеты речевые и видеоданные.

Услуга класса C является услугой с установлением соединений и предназначена для поддержки трафика с переменной скоростью передачи данных, не требующих поддержки синхронизации. Трафик, который использует услугу класса C, может включать, но не ограничен данными, предполагающими установление соединений, такими как кадры Frame Relay.

Услуга класса D поддерживает трафик данных, ориентированный на отсутствие соединений. Такой трафик характеризуется изменчивостью скорости передачи битов и отсутствием требований к сквозной синхронизации. Примером такого трафика являются пакеты протокола IP.

Четырем типам класса обслуживания первоначально соответствовали четыре типа протоколов адаптации ATM. Впоследствии протоколы AAL3 и AAL4 были заменены протоколом AAL3/4, который оказался неэффективным. Это привело к разработке нового протокола, получившего название SEAL (Simple Efficient Adaptation Layer – простой эффективный протокол адаптации). ATM-форум после принятия этого протокола дал ему название AAL5. Будущее, по-видимому, принадлежит AAL5.

2.2.3. Технология Ethernet

Сегодня более 85% локальных сетей выполнены по технологии канального уровня Ethernet. Отличительной особенностью канального уровня Ethernet является его разбиение на два подуровня: управления доступом к среде (Media Access Control, MAC) и управления логическим каналом (Logical Link Control, LLC). Подуровень MAC определяет алгоритм доступа к среде, адресацию рабочих станций в сети, а также поддерживает функции

совместного использования физической среды. Подуровень LLC поддерживает следующие службы:

– обслуживания без установления соединения и без подтверждения;

– обслуживания, ориентированного на соединение;

– обслуживания с подтверждением без установления соединения.

Главным недостатком технологии является конкурентный доступ к среде. В то же время это является и достоинством, позволяющим существенно уменьшить стоимость оборудования. При этом ограничения по дальности, традиционно относящие Ethernet к технологии локальных сетей, в случае использования ОВ снимаются: Ethernet становится технологией городских и глобальных сетей.

В своем развитии технология Ethernet прошла ряд эволюционных этапов (рис. 3.24) и из простой шинной архитектуры (10 Мбит/с Ethernet) превратилась в технологию реализации сегментов с увеличением скорости до 10 Гбит/с и более. При этом следует заметить, что пропускная способность Ethernet каждые 5-7 лет увеличивается в 10 раз. В настоящее время десятигигабитный Ethernet (Gigabit Ethernet, GE) использует технологию DWDM на физическом уровне.

В настоящее время GE прочно вошел в перечень базовых сетевых технологий для современных цифровых сетей. Технология GE прошла этап первичной стандартизации и представлена на рынке новейшей аппаратурой - маршрутизаторами/коммутаторами GE, выпускаемыми ведущими производителями ЦСП, и уже находит применение при построении современных высокоскоростных сетей передачи данных.

Интерфейс маршрутизаторов/коммутаторов GE 1000Base-X основывается на стандарте физического уровня Fibre Channel (FC) – технологии взаимодействия рабочих станций, суперкомпьютеров, устройств хранения и периферийных узлов, имеющей 4-уровневую архитектуру. Два нижних уровня FC-0 (интерфейсы и среда) и FC-1 (кодирование/декодирование) перенесены в GE, что значительно сократило время на разработку оригинального стандарта Gigabit Ethernet. В модели BOC/OSI стандарту GE соответствуют канальный и физический уровни.

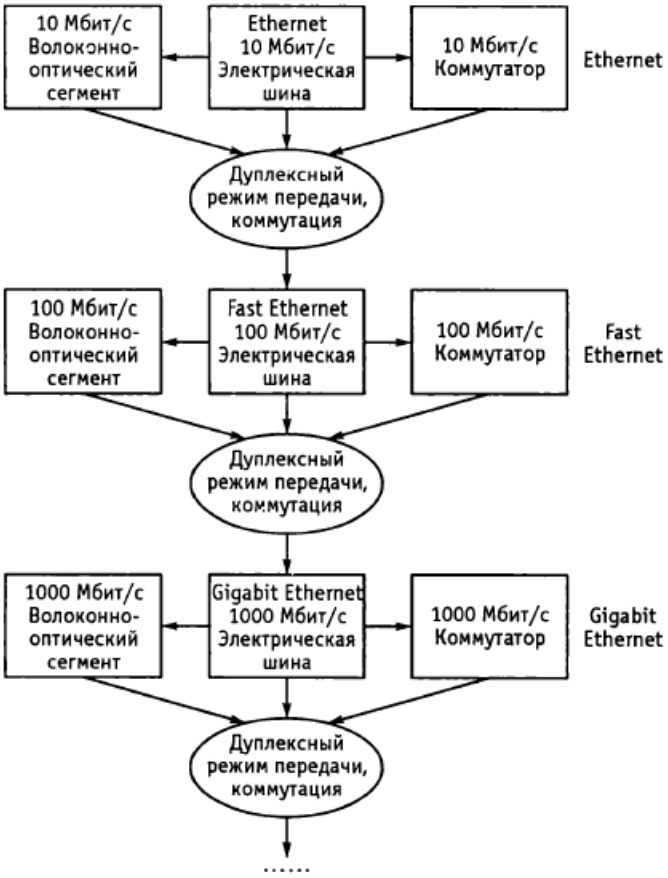


Рис. 3.24. Эволюция технологии Ethernet

Оборудование Ethernet всех поколений совместимо друг с другом и использует открытые стандарты. Поверх Ethernet возможна передача голоса, данных, видео. Технология многоадресной рассылки позволяет доводить до каждого пользователя неограниченное количество телевизионных и телефонных каналов, а скорость среды передачи данных дает возможность обеспечивать доступ пользователей к услугам на скоростях в сотни мегабит и гигабит в секунду уже сегодня.

Как отмечалось выше, большинство традиционных операторов используют в своих транспортных сетях технологию SDH. Отсюда вытекает вывод о целесообразности разворачивания мультисервисных сетей поверх существующих сетей SDH. Идея демонтировать SDH и перейти напрямую на ОВ с использованием WDM вряд ли кому то придет в голову, хотя бы из экономических соображений. Однако по своей идеологии мультисервисная сеть отличается от сети SDH, в первую очередь, по набору ориентированных на область применения функциональных свойств.

В данном случае наиболее проблемным является участок доступа. Развитие транспортной сети на этом участке обеспечивает задел для развития сети в будущем.

Операторам телематических служб, которые предоставляют в основном услуги широкополосной передачи данных и только начинают строить собственные транспортные сети, следует обратить внимание на технологии GE/10GE. В отличие от традиционных

операторов, компании, реализующие телематические услуги, обычно не имеют собственной инфраструктуры SDH, но располагают хорошо развитым участком доступа.

Рассмотрим далее отдельные вопросы, представление о которых необходимо иметь при выборе оборудования Ethernet поверх SDH (Ethernet over SDH).

Инкапсуляция Ethernet. Основная проблема инкапсуляции трафика Ethernet заключается в том, что блоки данных (контейнеры) SDH передаются безостановочно, независимо от наличия или отсутствия полезной нагрузки, в то время как кадры Ethernet передаются только при наличии нагрузки. Существует несколько процедур инкапсуляции трафика Ethernet в контейнеры SDH.

Стандартизованы процедуры GFP (Generic Framing Procedure – общая процедура кадрирования) и X.86 (известна как LAPS – протокол доступа к каналу SDH). Какая из них лучше? Обе инкапсулируют трафик Ethernet в контейнеры SDH, но по-разному. Процедура GFP выполняет инкапсуляцию более эффективно и, в отличие от LAPS, является детерминированной. Данные процедуры подробно описаны в стандартах ITU-T X.86 (LAPS) и ITU-T G.7041 (GFP). Отметим, что некоторые производители до сих пор используют свои собственные разработки.

Сцепка виртуальных контейнеров. Основной проблемой при передаче трафика Ethernet в сетях SDH является несогласованность скорости передачи кадров Ethernet с размерами контейнеров SDH.

Решить эту проблему помогает сцепка (concatenation) виртуальных контейнеров. Различают два вида сцепок: смежные (contiguous) и виртуальные (virtual). Виртуальная сцепка позволяет увеличивать пропускную способность сцепки виртуальных контейнеров с шагом VC-12 (2,176 Мбит/с), в то время как смежная сцепка может быть применена только начиная с уровня VC-4 (149,76 Мбит/с). Типы смежных и виртуальных сцепок представлены в табл. 3.8.

Нужно отметить, что при использовании виртуальных сцепок нет необходимости проводить какие-либо изменения в транзитных узлах существующей сети SDH, в то время как применение смежных сцепок требует замены оборудования всех транзитных узлов. Виртуальные сцепки имеют и другие достоинства, которые станут ясны, когда мы рассмотрим вопросы защиты трафика SDH. Все это позволяет утверждать, что следует использовать виртуальные сцепки контейнеров SDH. Процедура виртуальной сцепки описана в ITU-T H.707.

Регулирование емкости соединения. Функция автоматической защиты каналов SDH, описанная в документе ITU-T G.841, определяет три типа каналов:

– рабочий канал (если рабочее соединение по каким-либо причинам будет разорвано, трафик будет переключен на защитный канал в течение 50 мс);

– защитный канал - переносит трафик в случае отказа основного рабочего канала: данное соединение «простаивает», когда основной рабочий канал функционирует нормально, однако документ G.841 описывает использование защитного канала для передачи дополнительного трафика и в том случае, когда основной канал функционирует нормально;

– незащищенный канал.

Таблица 3.8. **Типы смежных и виртуальных сцепок**

SDH-контейнеры	Тип	Полезная нагрузка, Мбит/с
VC-12	Low Order	2,176
VC-3	High Order	48,384
VC-4	High Order	149,76
Contiguous Concatenation (смежная сцепка)		
VC-4-4c	High Order	599,04
VC-4-8c	High Order	1198,08
VC-4-16c	High Order	2396,16
VC-4-64c	High Order	9584,64
Virtual Concatenation (виртуальная сцепка)		
VC-12-Xv	Low Order	X·2,176 (X = 1...63)
VC-3-Xv	Low Order	X·48,384 (X = 1...255)
VC-4-Xv	High Order	X·149,76 (X = 1...255)

Потеря хотя бы одного незащищенного виртуального контейнера VC-12, входящего в виртуальную группу, приводит к потере всей группы. Для того чтобы этого не происходило, используется протокол LCAS (Link Capacity Adjustment Scheme - схема регулирования емкости соединения). Протокол LCAS выполняет функцию защиты трафика Ethernet, передаваемого по сетям SDH, и позволяет более гибко работать с этим трафиком.

Рассмотрим ситуацию, когда трафик передается с использованием нескольких каналов, объединенных в единую группу (рис. 3.25). При отказе незащищенного канала 1 трафик всей виртуальной группы будет потерян, но механизм LCAS отследит потерю соединения. Затем процедура GEP мгновенно изменит скорость и восстановит соединение с использованием оставшихся контейнеров, входящих в виртуальную группу. Это позволит задействовать каналы 2, 3 и 4 для передачи трафика без снижения отказоустойчивости сети. Время реакции LCAS для контейнеров VC-4 не превышает 64 мс, а для контейнеров VC-12 - 128 мс.

Как видно из данного примера, использование LCAS позволяет динамически распределять трафик между рабочими каналами, а также задействовать каналы защиты для передачи дополнительного трафика. Протокол LCAS описан в ITU-T G.7042.

Дополнительная функциональность Ethernet. Описанные выше возможности позволяют создать соединения Ethernet «точка-точка» E-line (рис. 3.26). Но это всего лишь выделенные каналы Ethernet, и не более того, сеть SDH является чистым транспортом для трафика Ethernet.

Строя сеть таким образом, оператор должен обеспечить число Ethernet-портов, равное числу соединений, а также использовать дополнительное оборудование для коммутации пакетов Ethernet. Кроме того, рано или поздно оператор столкнется с нехваткой ресурсов транспортной сети, хотя среднестатистическая загруженность каждого из каналов будет при этом мала. Следовательно, необходимо обеспечить возможность обработки пакетов Ethernet в соответствии с действующими стандартами (IEEE 802.1 D, 802.1 P и др.), что позволит более гибко работать с трафиком Ethernet и разделять его не только на уровне портов, как это делается сейчас многими операторами, но и на уровне Ethernet.

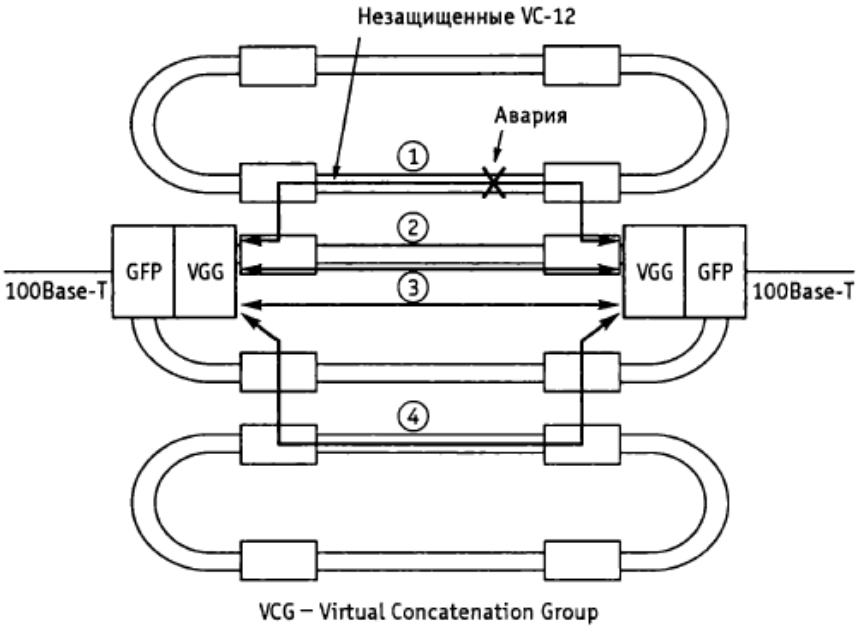


Рис. 3.25. Пример организации защиты трафика Ethernet с использованием технологии LCAS

Технология Ethernet позволяет разделять трафик абонентов или услуг в общем канале виртуальных локальных сетей (Virtual Local Area Network, VLAN). Большинство абонентов уже широко используют все достоинства данного метода, для реализации которого необходимо обеспечить беспрепятственную передачу идентификаторов VLAN через транспортную сеть. Механизмы создания собственных VLAN, а также приоритизации трафика Ethernet должны соответствовать существующим стандартам.

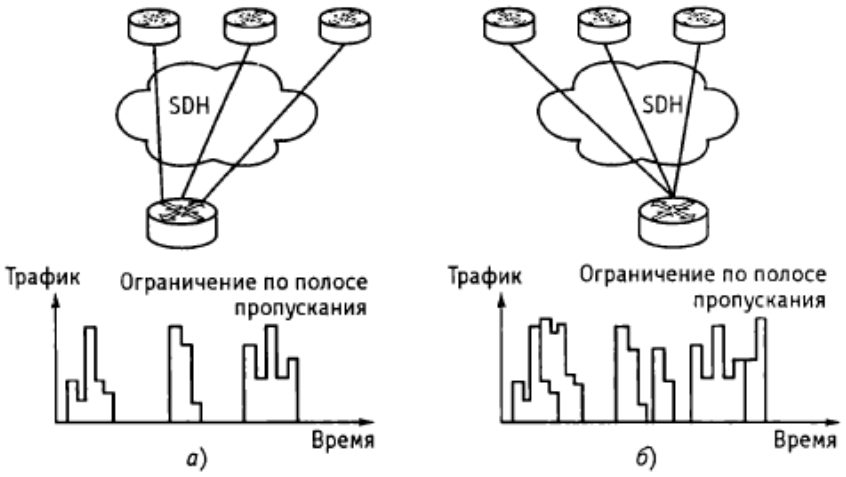


Рис. 3.26. Организация соединений:
а) «точка–точка»; *б*) «точка–много точек»

Все это позволяет строить сложные структуры «точка-много точек» и «много точек-много точек», известные как E-LAN (см. рис. 3.26), а также осуществлять концентрацию клиентского трафика и рационально использовать транспортную инфраструктуру.

Таким образом, следует обеспечить возможность полноценной работы с трафиком Ethernet в соответствии с рекомендациями IEEE 802.1 D (Bridge Protocol and Spanning Tree), IEEE 802.1 Q (VLAN) и IEEE 802.1 P (Priority).

Качество обслуживания. При увеличении числа обслуживаемых абонентов оператор сталкивается с проблемой обеспечения определенного качества обслуживания. Опыт зарубежных операторов показывает, что в ближайшее время функций Ethernet по обеспечению заданного в SLA (Service Level Agreement - договор об уровнях обслуживания) уровня обслуживания будет достаточно. Но в дальнейшем нужно будет дополнительно использовать возможности технологии MPLS (см. гл. 4).

Стек протоколов. Стек протоколов формируется следующим образом (рис. 3.27): абонент передает кадры Ethernet (с использованием или без использования собственных VLAN), которые инкапсулируются в кадры GFP, а они затем инкапсулируются в виртуальные сцепки контейнеров. Механизм LCAS обеспечивает защиту трафика Ethernet на случай возможных отказов путем динамического изменения пропускной способности соединения. SDH реализует взаимодействие на физическом уровне с существующими сетями.

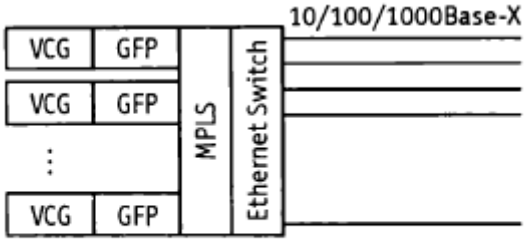


Рис. 3.27. Стек протоколов Ethernet-over-SDH
с использованием технологии MPLS

3. МНОГОПРОТОКОЛЬНАЯ КОММУТАЦИЯ ПО МЕТКАМ

3.1. Основы MPLS

Одним из перспективных направлений построения современной сетевой инфраструктуры является использование оптических технологий для организации высокоскоростной магистральной сети и единой системы сигнализации, позволяющей объединять различные типы сред и систем передачи информации. В качестве такой объединяющей технологии в настоящий момент рассматривается технология многопротокольной коммутации по меткам (Multiprotocol Label Switching, MPLS). Данная технология представляет собой попытку ускорить продвижение IP-пакетов и сохранить гибкость, характерную для IP-сетей, с помощью механизмов управления трафиком и поддержания качества обслуживания, применяющихся в сетях ATM. Внедрение технологии MPLS позволяет сохранить все лучшее, что присуще архитектуре IP-over-ATM (эффективное мультиплексирование и гибкость трафика, высокая производительность), и при этом она еще больше повышает масштабируемость сетей, упрощает их построение и эксплуатацию. Важно и то, что MPLS может использоваться не только с ATM, но и с любой другой технологией канального уровня. MPLS использует и развивает концепцию виртуальных каналов, используемых в сетях X.25, Frame Relay, объединяя ее с техникой выбора путей на основе информации о топологии и текущей загрузке сети, получаемой с помощью протоколов маршрутизации сетей IP. Это упрощает переход к следующему поколению волоконно-оптических магистралей Интернет на основе технологий SDH/WDM или IP/WDM.

MPLS - это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. MPLS сочетает в себе управление трафиком, характерное для технологий канального уровня, масштабируемость и гибкость протоколов сетевого уровня. «Многопротокольность» в названии технологии означает, что MPLS - инкапсулирующий протокол и может транспортировать множество других протоколов (рис. 4.1).

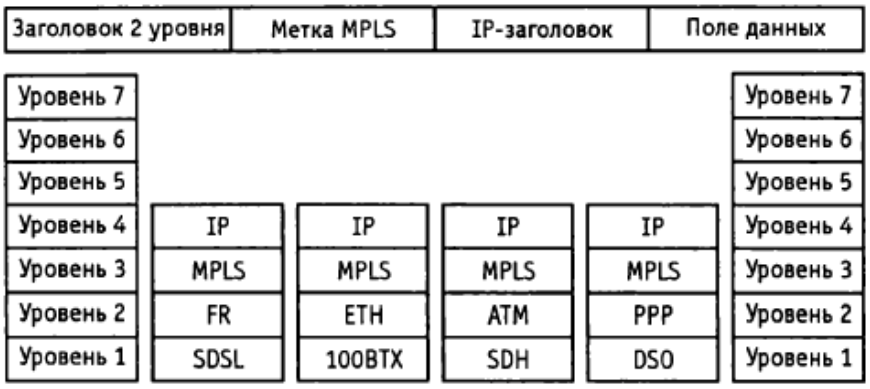


Рис. 4.1. Технология MPLS в IP-сетях и модель OSI/ISO

Сети ряда Интернет-провайдеров построены сегодня на основе многоуровневой модели, подразумевающей, что логическая маршрутизируемая IP-сеть функционирует поверх коммутируемой топологии второго уровня (ATM либо Frame Relay) и независимо от нее. Коммутаторы второго уровня обеспечивают высокоскоростные соединения, в то время как IP-маршрутизаторы на периферии сети, связанные друг с другом сетью виртуальных каналов второго уровня, осуществляют интеллектуальную пересылку IP-пакетов.

Таким образом, MPLS - это один из шагов на пути эволюционного развития сети Интернет в сторону упрощения ее инфраструктуры путем интеграции функций второго (коммутация) и третьего (маршрутизация) уровней.

В спецификации технологии MPLS заложен принцип разделения функций транспортировки потоков и управления ими (рис. 4.2). Отделение управляющей компоненты от пересылающей позволяет разрабатывать и модифицировать каждую из них независимо. Естественное обязательное требование состоит в том, чтобы управляющая компонента могла передавать информацию пересылающей компоненте через таблицу пересылки пакетов. Управляющая компонента задействует стандартные протоколы маршрутизации (OSPF, IS-IS, BGP-4) для обмена информацией с другими маршрутизаторами. На основе этой информации формируется и модифицируется сначала таблица маршрутизации, а затем, с учетом информации о смежных системах на каждом интерфейсе - таблица пересылки пакетов. Когда система получает новый пакет, пересылающая компонента анализирует информацию, содержащуюся в его заголовке, ищет соответствующую запись в таблице пересылки и направляет пакет на выходной интерфейс. Пересылающая компонента практически всех систем многоуровневой коммутации, включая и MPLS, основана на использовании последовательных меток пакетов. Метка - это короткое поле фиксированной длины в заголовке пакета.

С помощью MPLS можно решать следующие задачи:

- интеграцию ATM и Frame Relay с IP;
- ускоренное продвижение пакетов внутри сети оператора вдоль кратчайших традиционных маршрутов;
- создание виртуальных частных сетей (VPN);
- выбор и установление путей с учетом загрузки ресурсов (Traffic Engineering, TE).

Рис. 4.2. Функциональные компоненты маршрутизации

В книге не рассматриваются детально все возможности технологии MPLS. Желающие могут ознакомиться с ними сами. Мы ограничимся одним из наиболее важных применений технологии MPLS, а именно, службой VPN.

3.2. Элементы сети MPLS

В сетях, многопротокольной коммутации по меткам (MPLS-сетях), используются два вида сетевых узлов. Расположенные на границе сети MPLS маршрутизаторы должны распознавать и анализировать поступающие IP-потоки и направлять их по подходящим маршрутам. Эти устройства называются пограничными маршрутизаторами с коммутацией меток (Label Edge Router,LER). Различают входной и выходной LER.

Входной LER анализирует, как и обычный маршрутизатор, IP-заголовок и устанавливает, к какому классу эквивалентного обслуживания (Forwarding Equivalency Class, FEC) при выборе адреса следующей передачи пакета он принадлежит. FEC - класс пакетов сетевого уровня, которые получают от сети одинаковое обслуживание как при выборе пути продвижения пакета, так и с точки зрения доступа к ресурсам.

Абстрагирование отдельных пакетов в класс эквивалентности (или класс эквивалентного обслуживания, что одно и то же) FEC позволяет объединять большое количество потоков трафика, требующих одинаковой обработки. Объединенные в класс эквивалентности FEC потоки трафика идентифицируются одной и той же MPLS-меткой.

Возможность объединения потоков трафика независимо от адреса сетей назначения значительно увеличивает возможность MPLS к масштабированию за счет уменьшения

объема информации о маршрутах, хранимой и обрабатываемой маршрутизаторами коммутации меток (LSR-маршрутизаторами).

IP-дейтаграмма заключается в модуль данных протокола (Protocol Data Unit, PDU) технологии MPLS, а заголовок MPLS прикрепляется к дейтаграмме. Если заголовок объединен с операцией QoS (например, DiffServ), то входной LER будет рассматривать трафик в соответствии с правилами DiffServ. Далее LER принимает решение о выборе пути для данного пакета, посылая его к соответствующему транзитному маршрутизатору с коммутацией меток (Label Switch Routers, LSR). LSR получает PDU и использует заголовок MPLS для принятия решений пересылки. Он также производит замену меток. Данный LSR не занимается обработкой заголовка третьего уровня (IP-заголовка), а принимает решение о пересылке на основе метки пакета, а не на основе таблицы маршрутизации, и пересылает пакет дальше.

Далее, проходя, в общем случае, через несколько LSR, пакет попадает к выходному LER, который производит операцию разборки PDU, удаляет из пакета метку, анализирует заголовок пакета и направляет его к адресату, находящемуся вне MPLS-сети (рис. 4.3).

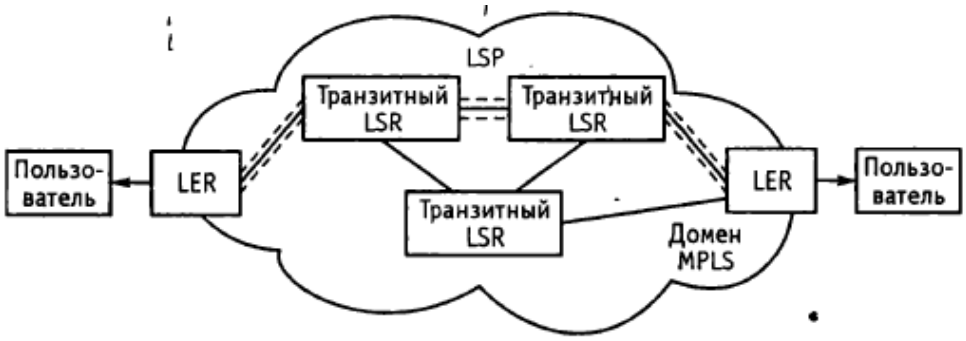


Рис. 4.3. Элементы сети MPLS

Пакеты, принадлежащие одному классу FEC, проходят путь от входного LER до выходного LER через множество транзитных LSR, образуя виртуальный коммутируемый по меткам тракт или путь (Label Switched Path, LSP). Установленное соединение является симплексным. Для организации полудуплексного соединения должны быть установлены два LSP. LSP всегда начинается на крае сети, заканчивается на противоположном конце, проходя через несколько транзитных маршрутизаторов.

3.3. Некоторые особенности технологии MPLS

3.3.1. Метки и способы маркировки

Метка - короткий идентификатор фиксированной длины, используемый на локальном участке сети, предназначен для определения класса эквивалентного обслуживания пакета при его пересылке по сети. На сегодняшний день стандартом определен формат 32-битной

метки, располагаемой между заголовками второго уровня (Layer 2) и третьего уровня (Layer 3). Для примера рассмотрим включение метки в IP-пакет заголовка Ethernet (рис. 4.4).

- Поле «Метка» - состоит из 20 бит и содержит собственное значение метки, используемое для определения маршрутизатора следующего шага, т. е. для продвижения пакетов.

- CoS (Class of Service) - поле необходимо для предоставления дифференциальных услуг в MPLS-сети. Для сквозного обеспечения QoS на границе MPLS-сети можно скопировать поле IP-приоритета в поле CoS. Поле состоит из 3 бит. Таким образом, в нем может передаваться только 3-битовое поле IP-приоритета, а 6-битового поля дифференцированной услуги (Differentiated Services Code Point, DSCP) - нет. При необходимости CoS может передаваться в виде одной из меток MPLS-стека. Поле метки способно вместить как поле IP-приоритета, так и поле DSCP.

- S - поле стека предназначено для поддержки иерархического стека меток. Бит S устанавливается в единицу для последней метки в стеке и в ноль для всех остальных меток стека. Это позволяет привязать префикс к нескольким меткам, другими словами - к стеку меток. Каждая метка стека имеет свои собственные значения поля CoS, S-бита и поле TTL.

- Время жизни (Time To Live , TTL) - 8 бит, используемых для кодирования количества ретрансляционных участков.

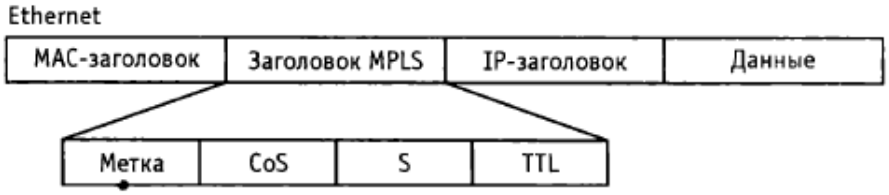


Рис. 4.4. Формат метки MPLS

Поле «Время жизни» является ключевым полем в заголовке IP-пакета. Обычно в объединенной IP-сети это поле уменьшается на единицу на каждом участке маршрута, и когда значение счетчика достигает нуля, пакет отбрасывается. Это делается для того, чтобы избежать зацикливания пакета или слишком долгого пребывания пакета в объединенной сети из-за неверной маршрутизации. Поскольку LSR не исследует IP-заголовок, поле времени жизни включается в метку, что позволяет сохранить функциональность этого поля.

Правила обработки поля времени жизни в метке:

1. Когда IP-пакет прибывает на входной пограничный маршрутизатор MPLS-домена (домен - это MPLS-сеть), в стек пакета помещается одна метка. Значение поля времени жизни этой метки устанавливается равным значению поля времени жизни IP-заголовка.

2. Когда MPLS-пакет прибывает на очередной транзитный маршрутизатор MPLS-домена, значение поля времени жизни в метке, находящейся на вершине стека, уменьшается на единицу.

- Если получившееся значение времени жизни нулевое, MPLS-пакет дальше не передается. В зависимости от значения метки в стеке, пакет либо просто отбрасывается, либо передается соответствующему «обычному» сетевому уровню для обработки ошибок (например, для формирования сообщения об ошибке с использованием протокола межсетевых управляющих сообщений – Internet Control Message Protocol, ICMP).

- Если получившееся значение времени жизни положительное, оно помещается в поле времени жизни в верхней записи стека для исходящего MPLS-пакета, после чего сам MPLS-пакет перенаправляется дальше. Исходящее значение поля времени жизни является функцией только входящего значения поля времени жизни и не зависит от того, были ли помещены в стек или извлечены из стека какие-либо метки до того, как переправить пакет дальше. Значения полей вре'мени жизни в записях, не находящихся на вершине стека, на ход обработки не влияют.

3. Когда MPLS-пакет прибывает на выходной пограничный маршрутизатор MPLS-домена, значение поля времени жизни, единственной находящейся в стеке записи, уменьшается на единицу, после чего метка извлекается из стека и стек меток становится пустым. В этом случае пакет выдается пользователю либо на сетевой уровень для обработки ошибок.

- Если получившееся значение положительное, оно помещается в поле времени жизни IP-заголовка, после чего IP-пакет перенаправляется дальше путем обычной маршрутизации. До того как переправить пакет дальше, должна быть пересчитана заново контрольная сумма IP-заголовка. Эта процедура необходима, чтобы убедиться, что повреждения заголовка не произошло при пересылке сообщения.

Использование меток значительно упрощает процедуру пересылки пакетов, так как маршрутизатор обрабатывает не весь заголовок IP-пакета, а только метку. Что занимает значительно меньше времени.

3.3.2. Стек меток

В рамках архитектуры MPLS вместе с пакетом разрешено передавать не одну метку, а несколько. При этом различают верхние и нижние метки:

- нижняя метка - будет обрабатываться самой последней по пути следования пакета;

- верхняя метка - обрабатывается самой первой по пути следования пакета.

Операции добавления/изъятия метки определены как операции на стеке. Результат коммутации задает лишь верхняя метка стека, нижние же передаются прозрачно до операции изъятия верхней.

Такой подход позволяет создавать иерархию потоков в сети MPLS и организовать туннельные передачи. Стек состоит из произвольного числа заголовков. Если стек меток имеет глубину т, то считается, что самая нижняя метка размещена на уровне 1, метка над ней

имеет уровень 2 и т.д., а метка наверху стека имеет уровень т. Верхняя метка в стеке находится ближе к заголовку сетевого уровня, а нижняя метка располагается ближе к заголовку канального уровня;

- CoS в стеках не используются.

Метка может принимать любое значение, кроме нескольких зарезервированных.

Пакет сетевого уровня следует сразу за записью стека с установленным в единицу битом S.

Записи стека меток располагаются после заголовка уровня передачи данных (канального уровня), но до заголовков сетевого уровня. В кадре протокола передачи данных (рис. 4.5, а), например протокола PPP (Point-to-Point Protocol - протокол точка-точка), стек меток располагается между IP-заголовком и заголовком уровня передачи данных.

В кадре сети стандарта IEEE 802 (рис. 4.5, б) стек меток располагается между IP-заголовком и заголовком уровня LLC (Logical Link Control - управление логическим соединением).

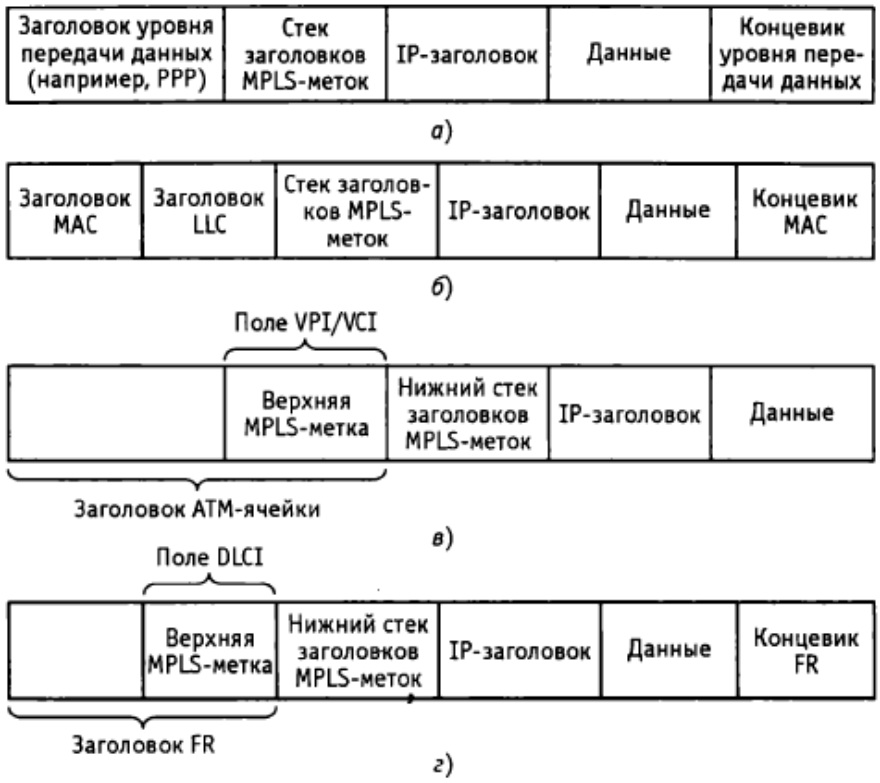


Рис. 4.5. *а*) Стеки заголовков меток MPLS в протоколе PPP; *б*) стек заголовков меток в кадре сети стандарта 802.x; *в*) стек заголовков меток MPLS в поле VPI/VCI; *г*) стек заголовков меток MPLS в поле DLCI

Если архитектура MPLS используется поверх ориентированной на соединение сетевой службы, может применяться другой подход, который иллюстрируют рис.4.5, в и г.

В ячейках ATM верхняя метка помещается в поле VPI/VCI в заголовке ячейки ATM. Верхняя метка остается на вершине стека, вставляемого между заголовком ячейки и IP-

заголовком. Помещение значения метки в заголовок ATM-ячейки упрощает работу ATM-коммутатора, которому по-прежнему достаточно просмотреть только заголовок ячейки.

Подобным же образом значение самой верхней метки может быть помещено в поле DLCI или в заголовке кадра FR (рис . 4.5, г). Необходимо обратить внимание, что в обоих случаях поле времени жизни остается невидимым для коммутатора и уменьшается на единицу по мере следования через транзитные узлы до станции назначения.

3.3.3. Классы эквивалентного обслуживания (FEC)

Классом эквивалентного обслуживания (Forwarding Equivalency Class,FEC) - называется группа пакетов третьего уровня, например IP-пакетов, которые одинаково обслуживаются и пересылаются. Термин FEC применяют для операций коммутации меткой. При использовании технологии MPLS соответствие между пакетом и «классом эквивалентного обслуживания» FEC устанавливается один раз, на входе в сеть MPLS. К одному FEC относятся пакеты всех потоков, пути следования которых через сеть (или часть сети) совпадают. С точки зрения выбора ближайшего маршрутизатора, к которому их надо переслать, все пакеты одного FEC неразличимы.

FEC используется для описания пакетов с адресом назначения, обычно адресом конечного получателя трафика, например хост-машины.

Использование FEC позволяет:

- Объединять пакеты в классы. При таком объединении значение FEC в пакете может использоваться для установки приоритетов. При обработке пакетов предоставляется более высокий приоритет одним пакетам по отношению к другим.

- Обеспечить поддержание эффективных операций QoS. Например, FEC могут быть связаны с высокоприоритетным голосовым трафиком в реальном времени, низкоприоритетным трафиком Интернет-конференций и т. д.

FEC-класс пакета может определяться по одному или по нескольким параметрам, указанным сетевым администратором. Среди возможных параметров можно назвать:

- IP-адрес отправителя и/или получателя или IP-адреса сетей;

- номера портов отправителя и/или получателя;

- идентификатор IP-протокола;

- код дифференцированной службы;

- метку потока IPv6.

Для различных классов обслуживания используются различные FEC и связанные с ними метки.

В сети MPLS возможны два подхода к пересылке пакетов с учетом класса обслуживания.

Таблица 4.1. **Пример связи адресов и FEC**

Адрес	FEC ID
120.166.4.8/4	A
177.200.7.8/3	B
202.240.76.9/1	C
387	D
474	E

Первый - предусматривает обработку пакетов в выходных очередях маршрутизаторов с учетом значений приоритета, указанного в заголовке MPLS.

Второй - базируется на том, что для каждой пары, состоящей из входного и выходного маршрутизаторов, определяется несколько путей коммутации меток (Label Switched Path, LSP) с различными характеристиками производительности, полосы пропускания, времени задержки и других параметров. После этого входной граничный маршрутизатор направляет один тип трафика по одному пути, другой – по другому, третий - по третьему и т.д.

В маршрутизаторах хранится таблица связи меток (Incoming Label Mapping, ILM). Для ее создания используется таблица переадресации помеченных пакетов (Next Hop Label Forwarding Entry, NHLFE). Производится обмен старой метки на новую, после чего пакет пересылается с новой меткой дальше. Эта процедура называется обменом меток. Одна входная метка может меняться на несколько исходящих меток. FEC является одним из основных компонентов MPLS, который определяет во многом работу всей сети. Все целевые адреса принадлежат к классам обслуживания FEC. FEC обычно ассоциируется напрямую с одним или несколькими адресами назначения. Эти данные записываются в таблицу маршрутизации. Если требуется направить поток данных к нескольким сетевым адресам одним и тем же путем, то для этих адресов выбирается один класс обслуживания. В простейшем случае записи не должны быть очень точными. Все пакеты с одной определенной сетью назначения ассоциируются с одним и тем же FEC. Также возможно один и тот же префикс относить к различным классам FEC. Назначение определенного FEC-класса должно выполнятся либо путем ручной настройки, либо с помощью сигнального протокола, либо на основе анализа пакетов, поступающих на входные маршрутизаторы.

Трафик одного FEC-класса пересекает MPLS-домен по LSP-пути.

Для определения топологии и текущего состояния домена требуется протокол маршрутизации, позволяющий каждому FEC-классу назначать конкретный LSP-путь. Протокол маршрутизации должен быть способен собирать и использовать информацию для поддержания требований к качеству обслуживания данного FEC-класса. Отдельные маршрутизаторы должны знать о LSP-пути данного FEC-класса, должны назначать LSP-путь входящей метке, а также должны обмениваться этой меткой со всеми остальными маршрутизаторами, которые могут послать им пакеты данного FEC-класса. LSP-пути классифицируются следующим образом:

- Между двумя граничными LER MPLS-домена проходит один маршрут.

- Один выходной LER, несколько входных маршрутизаторов. Назначенный одному FEC-классу трафик может поступать от разных источников через разные входные LER. Примером такой ситуации является корпоративная Интернет-сеть, расположенная в одном регионе, но с доступом к MPLS-домену через несколько входных LER. В такой ситуации через MPLS-домен проходит несколько маршрутов, возможно, с общими конечными ретрансляционными участками.

- Несколько выходных маршрутизаторов для трафика целевой рассылки. В рекомендации RFC 3031 утверждается, что чаще всего пакету присваивается FEC-класс на основе (частично или целиком) адреса получателя сетевого уровня. В противном случае, возможно, для FEC-класса потребуются маршруты к нескольким различным выходным маршрутизаторам. Однако, скорее всего, существует несколько сетей, в которые трафик может быть доставлен через один выходной LSR-маршрутизатор.

- В RFC 3031 групповая рассылка упоминается как предмет дальнейших исследований.

При создании сети нужно обратить внимание, чтобы число классов обслуживания было оптимальным для реализации всех важных приложений и требуемых параметров качества.

3.3.4. Таблицы

Для связи полученных меток с выходными метками используются различные таблицы и карты. Они предназначены для последующего управления стеками меток.

1. Таблица переадресации помеченных пакетов (Next Hop Label Forwarding Entry, NHLFE) - или строка пересылки следующего транзитного участка - используется, когда происходит пересылка пакета с меткой (табл. 4.2). Записи в таблице NHLFE содержат адрес следующего маршрутизатора и операции, которые необходимо совершить с данным пакетом:

- обмен внешней метки из стека;

- извлечение внешней метки из стека;

- обмен метки (т.е. каждый LSR после получения пакета изменяет значение метки прежде, чем послать пакет следующему LSR);

- вставка новой метки в стек.

Таблица 4.2. **Пример таблицы NHLFE**

NHLFE	Следующий LSR	Операция с меткой	Выходная метка	Исходящий порт
126	LSR C	Вставка	888	3821
546	LSR D	Обмен	777	7653
338	LSR F	Извлечение	–	–

Таблица 4.3. **FEC-to-NHLFE**

FEC	NHLFE
A	126
C	546
K	777

Таблица 4.4. **Пример таблицы Incoming Label Map (ILM)**

Label	NHLFE
888	126
777	546
555	757

Таблица также может содержать информацию о последовательности сборки пакета на канальном уровне и кодировании MPLS-заголовка стека.

Возможно, что принявший пакет маршрутизатор является последним на маркированном маршруте LSP. Тогда метка из пакета извлекается и пакет посылается дальше на основании решения третьего уровня эталонной модели ВОС (OSI).

2. Таблица связи (FEC-to-NHLFE, FTN) используется, если был принят пакет, не имевший до этого метки, но к которому была добавлена метка перед отправкой. В табл. 4.3. записано соответствие между каждым FEC и набором NHLFE. То есть карта FEC-to-NHLFE соотносит каждый класс FEC к множеству NHLFE, содержащих больше чем одну метку, но, прежде чем пакет будет послан, должна быть выбрана ровно одна метка множества.

3. Существует также карта входной метки (Incoming Label Map, ILM) - табл. 4.4. В ней находится связка к таблице NHLFE для пакетов, уже содержащих метку, т. е. протокол распределения меток (Label Distribution Protocol, LDP) записывает каждую входную метку в NHLFE. Если ILM вносит конкретную метку во множество NHLFE, то, прежде чем пакет будет отправлен, из стека должна быть выбрана ровно одна метка из множества. Метка в начале стека используется как индекс в ILM. Если ILM вносит метку во множество, содержащее больше чем один NHLFE, то это может быть полезно, если, например, она применяется для распределения нагрузки между различными каналами.

3.3.5. Правила назначения меток

На рис. 4.6 узлы A, B, G и H являются пользовательскими машинами и они не работают с MPLS. Узел C является входным LER, узлы D и E - транзитные LSR, а узел F - выходной LER. Информация передается пользователю узла G. Адрес этого узла может быть IP-адресом или некоторым другим адресом, например, IPX- или телефонным номером.

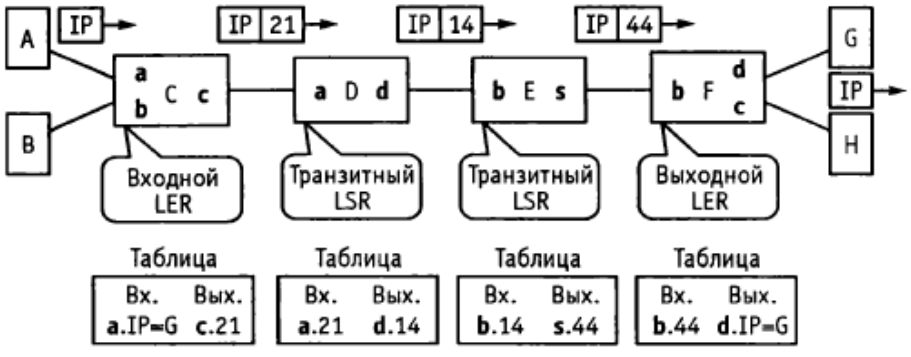


Рис. 4.6. Замена меток и пересылка

LER C получает IP-дейтаграмму, предназначенную для узла G, от узла A по интерфейсу a. LER C анализирует поля FEC, связывает FEC с меткой 21, вставляет дейтаграмму IP после заголовка метки и посылает пакет по выходному интерфейсу c. С учетом выходной строки в таблице NHLFE, LER C помещает метку 21 в заголовок метки в пакете. Производимая операция в LER C называется вводом метки.

Теперь LSR D и E обрабатывают только заголовок метки. Их таблицы замены меток используются (в LSR D) для замены метки 21 на метку 14, и для замены метки 14 на метку 44 (LSR E). Заметим, что данные таблицы используют входные и выходные интерфейсы на каждом LSR для связи меток с входными и выходными линиями передачи. Выходной LER F настроен так, что он распознает метку 44 по интерфейсу b как свою собственную метку. Далее выходная строка в таблице F указывает LER F послать дейтаграмму к G по интерфейсу d, что предполагает удаление метки из пакета.

Такое удаление метки является частью операции под названием вывод (выталкивание) метки.

3.4. Виртуальные частные сети MPLS (VPN MPLS)

VPN служит для организации прямого, безопасного соединения через общедоступный Интернет между клиентами (обычно конечным пользователем и корпоративным офисом) или между двумя ЛВС. Благодаря VPN удаленные пользователи могут обращаться к серверам предприятия и связываться с различными офисами своей компании. VPN может применяться как базовая архитектура обеспечения безопасности для экстрасети.

Для VPN не нужны выделенные линии, поэтому пользоваться ею может каждый, кто располагает доступом к Интернету. После того как соединение установлено, сотрудникам может предоставляться доступ ко всем ресурсам сети - так, словно они присутствуют в офисе. Самое большое достоинство технологии заключается в том, что, несмотря на общедоступную инфраструктуру, прямое соединение VPN, иногда именуемое «туннелем», защищено столь надежно, что украсть данные или получить несанкционированный доступ к территориально-распределенной сети становится очень трудно.

Сети VPN обладают рядом экономических преимуществ перед другими методами дистанционного доступа. Пользователи VPN могут обращаться к корпоративной сети, не устанавливая коммутируемое соединение, что позволяет сократить численность модемов или вообще отказаться от них. Можно обойтись и без выделенных линий, соединяющих удаленные офисы. Кроме того, повышается производительность труда, так как сотрудники могут пользоваться самыми быстрыми линиями связи, имеющимися в их распоряжении,

вместо того чтобы тратить время на установление коммутируемого соединения через банк модемов.

Компоненты MPLS VPN. Сеть MPLS VPN делится на две области: сети IP клиентов и внутренняя (магистральная) сеть MPLS провайдера, которая необходима для объединения сетей клиентов (рис. 4.7).

В общем случае у каждого клиента может быть несколько территориально обособленных сетей IP, каждая из которых в свою очередь может включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые «островки» корпоративной сети принято называть сайтами. Принадлежащие одному клиенту сайты обмениваются IP-пакетами через сеть провайдера и образуют виртуальную частную сеть этого клиента. Для обмена маршрутной информацией в пределах сайта узлы пользуются одним из протоколов IGP, OSPF или IS-IS, область действия которого ограничена автономной системой (набор сетей, которые находятся под единым управлением и совместно используют общую стратегию маршрутизации).

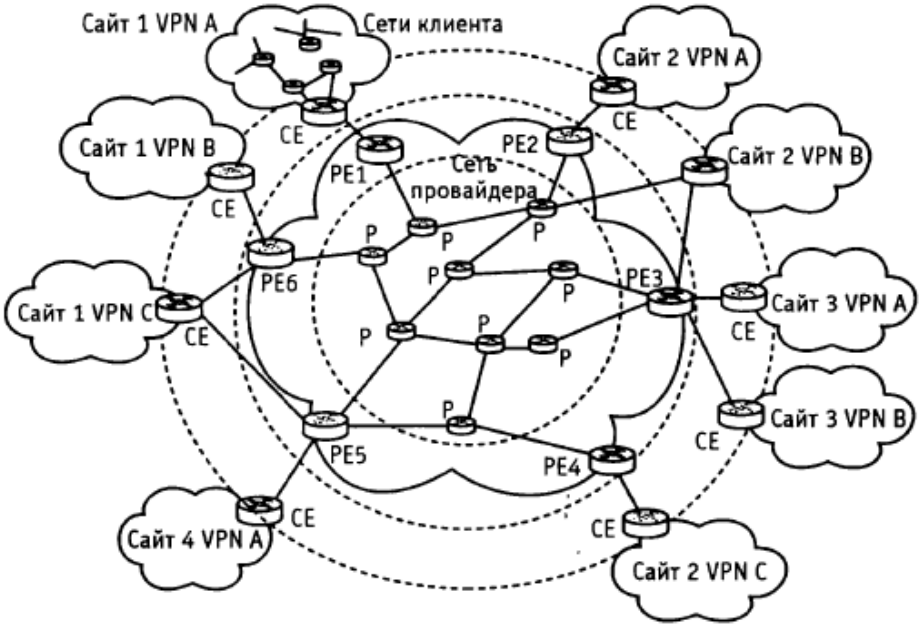


Рис. 4.7. Компоненты MPLS VPN

Маршрутизатор, с помощью которого сайт клиента подключается к магистрали провайдера, называется пограничным маршрутизатором клиента (Customer Edge router, CE). Будучи компонентом сети клиента, CE не имеет сведений о существовании VPN. Он может быть соединен с магистральной сетью провайдера несколькими каналами.

Магистральная сеть провайдера является сетью с технологией IP/MPLS, где пакеты IP продвигаются на основе не IP-адресов, а локальных меток. Сеть IP/MPLS состоит из маршрутизаторов с коммутацией меток (LSR), которые направляют трафик по предварительно проложенным путям с коммутацией меток (LSP) в соответствии со

значениями меток. Устройство LSR - это своеобразный гибрид маршрутизатора IP и коммутатора, при этом от маршрутизатора IP берется способность определять топологию сети с помощью протоколов маршрутизации и выбирать рациональные пути следования трафика, а от коммутатора - техника продвижения пакетов с использованием меток и локальных таблиц коммутации. Устройства LSR для краткости часто называют просто маршрутизаторами, и в этом есть свой резон - они с таким же успехом способны продвигать пакеты на основе IP-адреса, если поддержка MPLS отключена.

В сети провайдера среди устройств LSR выделяют пограничные маршрутизаторы провайдера (Provider Edge router, PE). Для их обозначения также используется аббревиатура LER (Label Edge Router).

К PE через маршрутизаторы CE подключаются сайты клиентов и внутренние маршрутизаторы магистральной сети провайдера (Provider router, P). Маршрутизаторы CE и PE обычно связаны непосредственно физическим каналом, на котором работает какой-либо протокол канального уровня - например, PPP, FR, ATM или Ethernet. Общение между CE и PE идет на основе стандартных протоколов стека TCP/IP, поддержка MPLS нужна только для внутренних интерфейсов PE (и всех интерфейсов P). Иногда полезно различать входной PE и выходной (удаленный) PE для определения направления продвижения трафика.

В магистральной сети провайдера только пограничные маршрутизаторы PE должны быть сконфигурированы для поддержки виртуальных частных сетей, поэтому только они «знают» о существующих VPN. Если рассматривать сеть с позиций VPN, то маршрутизаторы провайдера P непосредственно не взаимодействуют с маршрутизаторами заказчика CE, а просто располагаются вдоль туннеля между входным и выходным маршрутизаторами PE.

Маршрутизаторы PE являются функционально более сложными, чем P. На них возлагаются главные задачи по поддержке VPN, а именно, разграничение маршрутов и потоков данных, поступающих от разных клиентов. Маршрутизаторы PE служат также оконечными точками путей LSP между сайтами заказчиков, и именно PE назначает метку IP-пакету для его транзита через внутреннюю сеть маршрутизаторов P.

Таблица маршрутизации (VPN Routing and Forwarding, VRF).

Пути LSP могут быть проложены двумя способами: либо с применением технологии ускоренной маршрутизации (ЮР) с помощью протоколов LDP, либо на основе технологии трафик-инжиниринга (TE) с помощью протоколов RSVP. Прокладка LSP означает создание таблиц коммутации меток на всех маршрутизаторах PE и P, образующих данный LSP.

В совокупности эти таблицы задают множество путей для разных видов трафика клиентов. В VPN применяется различная топология связей: полносвязная, «звезда» (часто называемая в англоязычной литературе hub-and-spoke) или ячеистая (mesh).

Для корректной работы VPN требуется, чтобы информация о маршрутах через магистральную сеть провайдера не распространялась за ее пределы, а сведения о маршрутах в клиентских сайтах не становились известными за границами определенных VPN.

Барьеры на пути распространения маршрутных объявлений могут устанавливаться соответствующим конфигурированием маршрутизаторов. Протокол маршрутизации должен быть оповещен о том, с каких интерфейсов и от кого он имеет право принимать объявления определенного сорта и на какие интерфейсы и кому их распространять.

Роль таких барьеров в сети MPLS VPN играют пограничные маршрутизаторы PE или LER. Можно представить, что через маршрутизатор PE проходит невидимая граница между зоной клиентских сайтов и зоной ядра сети провайдера. По одну сторону располагаются интерфейсы, через которые PE взаимодействует с маршрутизаторами P, а по другую - интерфейсы, к которым подключаются сайты клиентов. С одной стороны, на PE поступают объявления о маршрутах магистральной сети, с другой стороны - объявления о маршрутах в сетях клиентов.

На рис. 4.8 показан маршрутизатор PE, на котором установлено несколько протоколов класса IGP. Один из них сконфигурирован для приема и распространения маршрутных объявлений только с тех трех внутренних интерфейсов, которые связывают этот PE с маршрутизаторами P. Два других протокола IGP обрабатывают маршрутную информацию от сайтов клиентов.

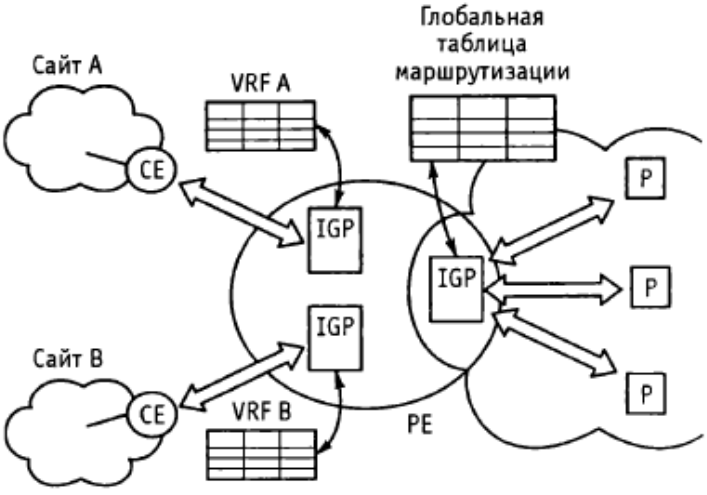


Рис. 4.8. Протоколы маршрутизации PE

Аналогичным образом настроены и остальные PE. Маршрутизаторы P принимают и обрабатывают маршрутную информацию IGP, поступающую со всех интерфейсов. В результате на всех маршрутизаторах PE и P создается по таблице маршрутизации, где содержатся все маршруты в пределах внутренней сети провайдера. Подчеркнем, что никакой информации о маршрутах в сетях клиентов в этих таблицах нет. Вместе с тем, и сети клиентов ничего не «знают» о маршрутах в сети провайдера. Таблица маршрутизации, создаваемая на пограничных маршрутизаторах PE на основе объявлений из магистральной сети, имеет специальное название «глобальная таблица маршрутизации». В отличие от нее таблицы, которые PE формирует на основе объявлений, поступающих из сайтов клиентов,

получили название таблиц VRF (VPN Routing and Forwarding). В VRF хранятся данные о маршрутах, информация о которых получена от клиентских маршрутизаторов.

Сайты клиентов представляют собой обычные сети IP, маршрутная информация в которых может передаваться и обрабатываться с помощью любого протокола маршрутизации класса IGP. Очевидно, что этот процесс никак не регламентируется провайдером. Маршрутные объявления свободно распространяются между узлами в пределах каждого сайта до тех пор, пока они не доходят до пограничных маршрутизаторов PE, служащих преградой для их дальнейшего распространения.

Разграничение маршрутов разных клиентов обеспечивает установка на маршрутизаторах PE отдельного протокола маршрутизации на каждый интерфейс, к которому подключен сайт клиента. Этот протокол принимает и передает клиентские маршрутные объявления только с одного, определенного для него интерфейса, не пересылая их ни на внутренние интерфейсы, через которые PE связан с маршрутизаторами P, ни на интерфейсы, к которым подключены сайты других клиентов. В результате на маршрутизаторе PE создается несколько таблиц маршрутизации VRF.

Несколько упрощая, можно считать, что на каждом PE создается столько таблиц VRF, сколько сайтов к нему подключено. Фактически на маршрутизаторе PE организуется несколько виртуальных маршрутизаторов, каждый из которых работает со своей таблицей VRF. Возможно и другое соотношение между сайтами и таблицами VRF. Например, если к некоторому PE подключено несколько сайтов одной и той же VPN, то для них может быть создана общая таблица VRF.

Объединение сайтов. Чтобы связать территориально разнесенные сайты заказчика в единую сеть, необходимо, во-первых, создать для них общее пространство распространения маршрутной информации, и, во-вторых, проложить во внутренней сети пути, по которым принадлежащие разным сайтам узлы одной и той же VPN могли вести обмен данными защищенным образом.

Механизмом, с помощью которого сайты одной VPN обмениваются маршрутной информацией, является многопротокольное расширение для BGP (Multiprotocol extensions for BGP-4, MP-BGP). С помощью этого протокола пограничные маршрутизаторы PE организуют взаимные сеансы и в рамках этих сеансов обмениваются маршрутной информацией из своих таблиц VRF.

Особенность протокола BGP и его расширений заключается в том, что он получает и передает свои маршрутные объявления не всем непосредственно связанным с ним маршрутизаторам, как протоколы IGP, а только тем, которые указаны в конфигурационных параметрах в качестве соседей. Маршрутизаторы PE сконфигурированы так, что все

получаемые от клиентских сайтов маршрутные объявления они адресно пересылают с помощью MP-BGP определенным пограничным маршрутизаторам PE. Вопрос о том, кому отправлять маршрутные объявления, а кому нет, целиком зависит от топологии виртуальных частных сетей, поддерживаемых данным провайдером. Так, на рис. 4.7 маршрутизатор PE1 передает маршруты из таблицы VRF сайта 1 в VPN A на маршрутизаторы PE2, PE3, PE5, к которым подключены остальные сайты 2, 3 и 4 той же VPN A. Полученный маршрут заносится в таблицу VRF соответствующего сайта.

Таким образом, кроме маршрутов, поступающих от непосредственно подсоединенных к PE сайтов, каждая таблица VRF дополняется маршрутами, получаемыми от других сайтов данной VPN по протоколу MP-BGP. Целенаправленное распространение маршрутов между маршрутизаторами PE обеспечивается надлежащим выбором атрибутов протокола MP-BGP.

Независимость адресных пространств. Если некоторое множество узлов никогда, ни при каких условиях, не получает маршрутную информацию от другого множества узлов, то адресация узлов в пределах каждого из этих множеств может выполняться независимым образом.

Ограничение области распространения маршрутной информации пределами отдельных VPN изолирует адресные пространства каждой VPN, позволяя применять в ее пределах как адреса Internet общего пользования, так и частные (private) адреса, зарезервированные в соответствии с RFC 1819.

Почему же в таком случае не сделать выбор адресов в пределах VPN совершенно произвольным и ограниченным только общими правилами адресации стека TCP/IP? Дело в том, что во многих случаях клиенты не хотят полной изоляции VPN: в частности, они нуждаются в выходе в Интернет. Независимое же, не согласованное с регламентирующими органами Интернет, назначение адресов узлам VPN может привести к совпадению внутренних адресов сайтов с уже выделенными адресами общего пользования, в результате чего связь с Интернет общего пользования станет невозможной. При использовании зарезервированных частных адресов проблема связи клиентов VPN с внешним миром решается с помощью стандартной техники трансляции адресов (Network Address Translator, NAT), описанной в RFC 3022. В любом случае должно соблюдаться требование уникальности адресов в пределах VPN.

Использование в разных VPN одного и того же адресного пространства создает проблему для маршрутизаторов PE. Протокол BGP изначально был разработан в предположении, что все адреса, которыми он манипулирует, во-первых, относятся к семейству адресов IPv4 и, во-вторых, однозначно идентифицируют узлы сети, т.е. являются глобально уникальными в пределах всей составной сети. Ориентация на глобальную уникальность адресов выражается

в том, что, получив очередное маршрутное объявление, протокол BGP анализирует его, не обращая внимания на то, какой VPN принадлежит этот маршрут. Если на вход BGP поступают описания маршрутов к узлам разных VPN, но с совпадающими адресами IPv4, то BGP считает, что все они ведут к одному и тому же узлу, а, следовательно, как и полагается в таком случае, он помещает в соответствующую таблицу VRF только один кратчайший маршрут.

Проблема решается за счет применения вместо потенциально неоднозначных адресов IPv4 расширенных и однозначных адресов нового типа, а именно, адресов VPN-IPv4, получаемых в результате преобразования исходных адресов IPv4. Преобразование заключается в том, что ко всем адресам IPv4, составляющим адресное пространство той или иной VPN, добавляется префикс, называемый различителем маршрутов (Route Distinguisher, RD), который уникально идентифицирует эту VPN. В результате на маршрутизаторе PE все адреса, относящиеся к разным VPN, обязательно будут отличаться друг от друга, даже если они имеют совпадающую часть - адрес IPv4.

Именно здесь оказалась полезной способность расширенного протокола MP-BGP переносить в маршрутных объявлениях адреса разных типов, в том числе IPv6, IPX, а, главное, VPN-IPv4. Адреса VPNIPv4 используются только для маршрутов, которыми маршрутизаторы PE обмениваются по протоколу BGP. Прежде чем передать своему напарнику некоторый маршрут, входной маршрутизатор PE добавляет к его адресу назначения IPv4 префикс RD для данной VPN, тем самым преобразуя его в маршрут VPN-IPv4.

Как уже было сказано, различители маршрута должны гарантированно уникально идентифицировать VPN, чтобы избежать дублирования адресов. Упростить выбор RD, не создавая для этих целей дополнительных централизованных процедур (например, распределения RD органами Интернет подобно распределению адресов IPv4), предлагается за счет использования в качестве основы для RD заведомо уникальных чисел - либо номеров автономных систем, либо глобальных адресов интерфейсов PE с магистральной сетью провайдера (в сети провайдера всегда необходимы глобальные адреса для взаимодействия с сетями других провайдеров).

Различитель маршрутов RD имеет длину 8 байтов и состоит из трех полей. Первое поле Type длиной 2 байта определяет тип и разрядность второго поля, которое называется Administrator и однозначно идентифицирует провайдера. Значение 0 поля Type говорит о том, что в поле Administrator указывается IP-адрес интерфейса маршрутизатора PE, и длина данного поля составляет, естественно, 4 байта. Если же значение Type равно 1, то в качестве идентификатора провайдера выбрано значение номера его автономной системы, так что

длина поля Administrator составит уже 2 байта. Третье поле носит название Assigned Number, его назначение - обеспечить уникальность адресов VPN в пределах сети провайдера. Значения поля Assigned Number выбирает сам провайдер, при этом использование в качестве поля Administrator IP-адресов интерфейса PE более удобно, так как ограничивает требование уникальности значений Assigned Number пределами отдельного PE.

Документ RFC 2547bis не требует, чтобы все маршруты внутри одной VPN индексировались одним и тем же значением RD. Более того, один и тот же сайт, подключенный к разным интерфейсам одного PE или к разным PE, может иметь различающиеся RD. Благодаря этому путь к одному и тому же узлу может описываться разными маршрутами, что дает возможность выбора того или иного маршрута для различных пакетов. Однако принципиально важно, чтобы RD разных VPN не совпадали.

Пересылка пакета по сети MPLS VPN. Пусть, например, из сайта 1 в VPN A узел с адресом 10.2.1.1/16 (16 - класс эквивалентности при доставке FEC) отправляет пакет узлу сайта 2 этой же VPN, имеющему адрес 10.1.0.3/16 (рис. 4.9). Стандартными транспортными средствами IP-пакет доставляется на пограничный маршрутизатор сайта CE1A, в таблице которого для номера сети 10.1.0.0 в качестве следующего маршрутизатора указан PE1. На маршрутизатор PE1 пакет поступает с интерфейса int2, поэтому для выбора дальнейшего продвижения пакета он обращается к таблице VRF 1A, связанной с данным интерфейсом.

В таблице VRF 1A адресу 10.1.0.0 соответствует запись протокола BGP, которая указывает, 4to очередным маршрутизатором для пакета определен PE2. Следующее поле записи содержит значение метки Lvpn = 7, определяющей интерфейс выходного маршрутизатора PE, которое должно быть присвоено пакету для того, чтобы он попал в нужную VPN. Здесь также указывается, что запись была сделана протоколом BGP, а не IGP. На этом основании маршрутизатор PE «понимает», что очередной маршрутизатор не является непосредственным соседом, и путь к нему надо искать в глобальной таблице маршрутизации.

В глобальной таблице для адреса PE2 указывается начальное значение метки L пути LSP, равное 3. Способ его прокладки между маршрутизаторами PE1 и PE2 не имеет в данном случае принципиального значения - главное, чтобы такой путь существовал.

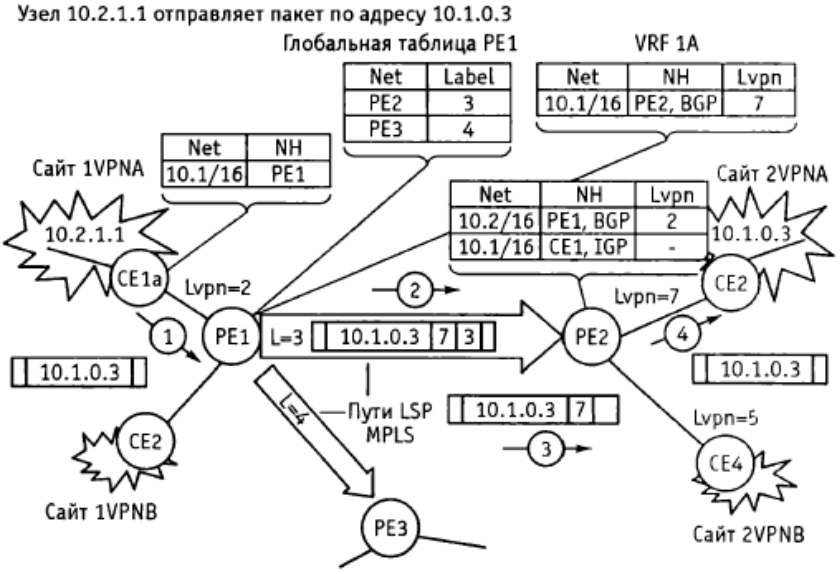


Рис. 4.9. Путешествие пакета между сайтами VPN

Технология MPLS VPN использует иерархические

свойства путей MPLS, за счет чего пакет может быть снабжен несколькими метками, помещаемыми в стек. На входе во внутреннюю сеть провайдера, образуемую маршрутизаторами P (LSR), пакет будет снабжен двумя метками - внутренней Lvpn = 7 и внешней L = 3. Метка Lvpn интерпретируется как метка нижнего уровня - оставаясь на дне стека, она не используется, пока пакет путешествует по туннелю PE1-PE2. Продвижение пакета происходит на основании метки верхнего уровня, роль которой отводится метке L. Каждый раз, когда пакет проходит очередной маршрутизатор P вдоль туннеля, метка L анализируется и заменяется новым значением. И только после достижения конечной точки туннеля маршрутизатора PE2 из стека извлекается метка Lvpn. В зависимости от ее значения пакет направляется на тот или иной выходной интерфейс маршрутизатора PE2.

Из таблицы VRF 2A, связанной с данным интерфейсом и содержащей маршруты VPNA, извлекается запись о маршруте к узлу назначения, указывающая на CE2 в качестве следующего маршрутизатора. Заметим, что она была помещена в таблицу VRF 2A протоколом IGP. Последний отрезок путешествия пакета от CE2 до узла 10.1.0.3 осуществляется традиционными средствами IP.

Несмотря на достаточно громоздкое описание механизмов MPLS VPN, процесс конфигурирования новой VPN или модификации существующей достаточно прост, поэтому он хорошо формализуется и автоматизируется. Для исключения возможных ошибок конфигурирования - например, приписывания сайту ошибочной политики импорта/экспорта маршрутных объявлений, что может привести к присоединению сайта к чужой VPN, - некоторые производители разработали автоматизированные программные системы конфигурирования MPLS. Примером может служить Cisco VPN Solution Center, который снабжает администратора средствами графического интерфейса для формирования состава каждой VPN, а затем переносит полученные конфигурационные данные в маршрутизаторы PE.

Повысить степень защищенности MPLS VPN можно с помощью традиционных средств: например, применяя средства аутентификации и шифрования IPSec, устанавливаемые в сетях клиентов или в сети провайдера. Услуга MPLS VPN может легко интегрироваться с другими услугами IP, например, с предоставлением доступа к Интернет для пользователей VPN с защитой их сети средствами межсетевого экрана, установленного в сети провайдера. Провайдер также может предоставлять пользователям MPLS VPN услуги, базирующиеся на других возможностях MPLS: в частности, услуги с предоставлением гарантированного качества обслуживания на основе методов MPLS TE. Что же касается сложностей ведения в маршрутизаторах провайдера таблиц маршрутизации пользователей, на которые указывают некоторые аналитики, то они несколько преувеличены, так как таблицы создаются

автоматически, с помощью стандартных протоколов маршрутизации, и только на пограничных маршрутизаторах PE. Механизм виртуального маршрутизатора полностью изолирует эти таблицы от глобальных таблиц маршрутизации провайдера, что обеспечивает необходимые уровни надежности и масштабируемости решений MPLS VPN.

3.5. Обобщенная многопротокольная коммутация по меткам (GMPLS)

Технология обобщенной (универсальной) многопротокольной коммутации по меткам (Generalized Multi-Protocol Label Switching, GMPLS) была разработана технической комиссией Интернет (Internet Engineering Task Force, IETF). В проекте стандарта GMPLS говорится:

«Сети будущего будут состоять из таких систем, как маршрутизаторы, DWDM системы, Add-Drop мультиплексоры (ADMS), фотонные (PXCs) или оптические коммутаторы (OXCs), которые будут использовать GMPLS».

В GMPLS используются концепции и протоколы, разработанные применительно к MPLS. В GMPLS принцип коммутации по меткам расширен применительно к оптическим сетям. Здесь, в отличие от MPLS, вместе с меткой необходимо передавать информацию о ее типе, поскольку в качестве меток могут быть выбраны различные компоненты - длина волны λ, номер оптического волокна в канале, номер SDH-контейнера и т.д. В настоящий момент предложены следующие базовые типы меток:

- Packet - метка, идентифицирующая Ethernet (GE, FE);
- PDH - метка, идентифицирующая кадры ETSI/ANSI POH (T1, E1, E3);
- SONET/SDH - метка, идентифицирующая контейнеры SONET/SDH (VT, VC, STS-n, STM-n);
- Digital Wrapper - метка OTN G.709 (2,5,10, 40 Гбит/с);
- λ - длина волны при использовании фотонных λ-коммутаторов OXC;
- Fiber - метка, идентифицирующая номер оптического волокна;
- Fiber Channel - метка, идентифицирующая оптический канал.

Перечисленные выше типы меток описывают тип устанавливаемого соединения LSP, а не транспортной технологии, через которую данный LSP устанавливается. Например, использование метки X означает, что устанавливаемое соединение LSP следует обеспечивать прозрачно без оптико-электрических преобразований. Тип метки Ethernet означает, что следует также обеспечить синхронизацию и, возможно, согласование скоростей на транзитных коммутаторах. В свою очередь, при запросе, например метки SONET/SDH, необходимо указывать тип и количество контейнеров.

GMPLS эволюционировала от MPLS (через MPA.S) путем расширения существующей парадигмы коммутации по меткам, от технологий коммутации пакетов/ячеек/фреймов к технологиям, ориентированным на установление соединения. Хотя принцип коммутации по меткам был изначально внедрен для повышения скорости маршрутизации в IP-сетях (посредством исключения трудоемкого сравнения полных префиксов), акцент сместился в сторону увеличения стабильности, улучшению QoS и более гибким и эффективным механизмам управления (возможных благодаря улучшенному планированию трафика).

GMPLS охватывает всю сферу коммутационных возможностей: от коммутации пакетов до коммутации оптических волокон. GMPLS не только использует концепцию MPLS (например, планирование трафика MPLS и восстановление), но и базируется на тех же протоколах маршрутизации (например, OSPF-TE) и сигнализации (RSPV-TE).

Фундаментальная концепция GMPLS (интегрированная плоскость управления, (многоуровневое) восстановление, и распределенное управление) могут быть применены для устранения недостатков существующих технологий для многоуровневых сетей. Повышенная гибкость сети, обеспечиваемая GMPLS, может повысить доходы операторов, так как они могут предложить и твердо придерживаться более строгих (и более прибыльных) соглашений об уровне обслуживания (SLA). А благодаря оптимизированному распределению ресурсов восстановления и эффективным (многоуровневым) механизмам восстановления, можно снизить капитальные затраты (CAPEX). К тому же, автоматическое восстановление - с исключением необходимости в дорогостоящих и вносящих ошибки ручных вмешательствах – может снизить эксплуатационные расходы (OPEX).

Улучшенные возможности- QoS позволяют эффективно передавать через единую сеть сообщения с различными классами обслуживания (Class of Service, CoS), такие, как голос, видео, и данные с их специфическими требованиями в плане задержки, джиттера и доступности. Гибкое и эффективное сетевое управление, предоставленное унифицированной плоскостью управления GMPLS, позволяет быстрее и проще вводить (новые) услуги, что также приводит к увеличению прибылей (более ранней тарификации услуг) и снижению эксплуатационных затрат (OPEX) благодаря упрощенному сетевому управлению.

4. ОБЪЕДИНЕНИЕ ТРАДИЦИОННОЙ ТЕЛЕФОННОЙ СЕТИ И ПАКЕТНОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИИ SOFTSWITCH

Сеть сигнализации является основой для всех телекоммуникационных служб, находящихся в сетях разных типов. И хотя сигнальная архитектура интеллектуальных сетей будущего полностью не определена, некоторые ее важные черты ясны уже сегодня. Так, она будет поддерживать разнообразные протоколы, чтобы операторы смогли оказывать многочисленные новые услуги в интеллектуальных сетях, построенных с использованием унаследованной инфраструктуры. «Стандартный» набор возможностей, которыми обладает классическая сигнализация телефонных сетей общего пользования (ТфОП) - обнаружение неисправностей, разделение сигнальной нагрузки, распределенный интеллект, будет усилен за счет масштабируемости, быстродействия и экономичности пакетных сетей.

В сетях будущего важную роль сохранит сигнализация ОКС №7. Она будет отвечать за перенаправление вызова, запоминание данных о вызове и другие функции обработки вызовов, работу бизнес-приложений - расчет с абонентами (биллинг), индивидуальное обслуживание абонентов и т.д., а также за предоставление многих услуг нового поколения - уведомление абонента, работающего on-line, о поступлении вызова, оказание услуг по предоплате, навигацию в Интернет при подключении on-line по беспроводной сети и др. В то же время комбинация технологий IP и ОКС № 7 на уровне сигнальной сети позволит операторам воспользоваться преимуществами сетей обоих типов: сохранить инвестиции, вложенные в построение инфраструктуры интеллектуальных сетей (IN), и перейти к конвергированным сетям, использующим протоколы сигнализации для передачи голоса через IP. В конвергированных сетях IP-технологии помогут поддерживать сеансы мультимедиа, новые режимы доступа абонентов, новые услуги, более эффективно использовать полосу пропускания и, как результат, значительно снизить расходы операторов.

Стыковка сетей традиционной телефонии с сетями пакетной коммутации в современных конвергированных сетях осуществляется на основе общей сигнальной сети, обеспечивающей независимое управление передачей информации и соединяющей разнородные сети. Общая сигнальная сеть позволяет провайдерам оказывать услуги, присущие ТфОП, с гибкостью и эффективностью, которые свойственны пакетным сетям.

Современная инфраструктура сигнальных сетей развивается в направлении распределенной архитектуры, которая основана на использовании технологии Softswitch.

По мере того как интеллект сигнальной сети будет возрастать, сети сигнализации начнут приближаться к информационным системам, решающим задачи сетевого планирования, предотвращения мошенничества, расчетов с абонентами, гарантированного предоставления услуг и поддержки других бизнес-приложений, а операторы инфраструктуры станут широко применять методы искусственного интеллекта для анализа сигнальной информации.

4.1. Оборудование для сетей на основе Softswitch от компании ZTE

Компания ZTE считает целесообразным использовать оборудование Softswitch прежде всего для построения NGN классов 4 и 5. NGN класса 4 (тандемного типа) предоставляет абонентам услуги передачи голоса и данных: местные и междугородные соединения VoIP между абонентами ТфОП и услуги ПД по сети IP. В NGN класса 4 отсутствуют коммутаторы ТфОП с входящими интерфейсами соединительных линий, а подключение ТфОП к IP-сети осуществляется с помощью сигнального и транспортного шлюзов. NGN класса 5 будет предоставлять услуги VoIP, что позволяет избежать крупных инвестиций для построения телефонных узлов и ПД. Исключены любые коммутаторы ТфОП, а медные пары абонентов подключаются непосредственно к шлюзам NGN или устройствам интегрированного доступа.

NGN классов 4 и 5 предложат абонентам большой набор услуг, что делает технологию Softswitch весьма привлекательной для операторов и сервис-провайдеров.

Компания выделяет следующие технологические преимущества своего оборудования:

1. Полностью конвергированные услуги передачи голоса и данных в IP-сети, возможность подключения к ТфОП. Высокие показатели QoS голосовой связи.

2. Высокая производительность - поддержка более 2 млн соединений в ЧНН при использовании одного контроллера Softswitch и более 6 млн. соединений при каскадном соединении трех котроллеров.

3. Гибкие сетевые решения для построения NGN класса 4 (услуги междугородной связи) и класса 5 (услуги местной связи с помощью устройств интегрированного доступа IAD).

4. Возможность сохранения коммутаторов ТфОП путем подключения NGN к ТфОП с помощью сигнального и транспортного шлюзов.

5. Надежная система управления NGN.

6. Разумные цены и четкое обслуживание абонентов.

Таблица 5.1. **Проекты компании ZTE**

Операторы	Количество абонентов	Трафик, мин./день	Стоимость, долл./мин.
China Netcom	21 000	170 000	0,03…0,04
China Unicom	Коммерческое тестирование с 1000 абонентов		
China Railway	Коммерческое тестирование с 1000 абонентов		
China Telecom	> 6000 абонентских линий в 400 IP phone 150 000 1. ZTE, Huawei, Alcatel, Cisco и VocalTel приняли участие в первом этапе тендера по проекту TT&T NGN 2. ZTE и Huawei вышли на второй этап тендера. Softswitch от ZTE прошел все виды тестирования для TT&T. В настоящее время ZTE и TT&T ведут переговоры о дальнейшем сотрудничестве		
Thailand TT&T Project			
Hong Kong Wharf NGN	1. ZTE и Lucent и Nortel приняли участие в первом этапе тендера по проекту Hong Kong Wharf NGN 2. ZTE и Nortel вышли на второй этап тендера. Softswitch от ZTE прошел все тесты для Hong Kong Whart NGN project. В настоящее время ZTE и Hong Kong Wharf NGN ведут переговоры о дальнейшем сотрудничестве		
Philippine Digital NGN	1. ZTE, Huawei, Cisco, Alcatel, UT, Ericsson и Sandra приняли участие в первом этапе тендера по проекту Digital NGN 2. ZTE, Huawei и Cisco вышли на второй этап тендера		
Romania RPO NGN	ZTE – единственный победитель тендера по проекту Romania RPO NGN		

Компания имеет большой опыт реализации NGN проектов (табл. 5.1).

Достоинством оборудования Softswitch, производимого компанией ZTE, является его совместимость с оборудованием других вендоров (табл. 5.2).

Отметим также, что решения ZTE предусматривают интеграцию оборудования с интеллектуальными и мобильными платформами. Так, Softswitch ZTE может использоваться в качестве виртуального SSP (пункта коммутации услуг IN) с поддержкой INAP/TCAP. Пока Softswitch соединяется с мобильными платформами через ТфОП, однако в ближайшее время планируется выпуск проводно-беспроводного контроллера Softswitch, интегрированного с мобильными платформами и работающего в ядре сети ЗС.

Таблица 5.2. **Совместимость оборудования**

Вендор	Оборудование	Протокол взаимодействия
Протестировано взаимодействие со следующими Softswitch		
Lucent Softswitch SIP-T		
SS8 SGS SIP-T		
Cisco SIP Proxy SIP		
Siemens Softswitch SIP-T		
Nortel Softswitch SIP-T		
Протестировано взаимодействие со следующими транспортными шлюзами		
Audiocodes MP108, MP100, MP200 MGCP		
InnoMedia MTA3328-4 MGCP		
TAINET VENUS2804 MGCP		
CodentNetworks CS2912 MGCP		
Протестировано взаимодействие со следующими терминалами		
3COM Sip phone SIP		
Pingtel Sip phone SIP		
Welltech Sip phone SIP		
Cisco Sip phone SIP		
Cisco ATA 186 SIP		
PhotonicBridges P103 MGCP		
ACT P103B H.248		
Leadtek BVP8770 (Video Phone) H.323		
INNOmedia MTA3368 (Video Phone) SIP		

В заключение заметим, что Softswitch производства ZTE отвечает требованиям COPM, а NGN ZTE включает в себя систему управления сетью (NMS) для авторизации всех устройств, находящихся под управлением контроллера Softswitch. Опорная сеть IP имеет и другие системы защиты от атак хакеров: брандмауэры, сообщения (traps) SNMP, системные журналы регистрации.

4.2. Примеры использования Softswitch компании ZTE на сетях NGN

4.2.1. Развертывание NGN класса 5 для China Netcom

В августе 2001 г. корпорация ZTE успешно завершила строительство сети NGN на основе Softswitch для компании China Netcom. Это была первая в мире NGN на основе Softswitch, и после ее расширения она стала одной из самых крупных в мире NGN класса 5 (рис. 5.18). На первом этапе производимые ZTE устройства управления Softswitch (ZXSS10 SS1), транковый шлюз TG (ZXSS10 M100) и шлюз сигнализации SG (ZXSG10) устанавливались и конфигурировались на центральной станции с терминалами нескольких типов, такими как интегрированное устройство доступа (IAD), MP100 от Audio Codes и SIP-телефон от PingTel.

SG и TG были подключены к PSTN через фронтальный процессор компании Netcom. На этом этапе были проведены всесторонние испытания системы Softswitch от ZTE с точки зрения рабочих характеристик вызовов.

На втором этапе в жилых домах, в некоторых жилых зонах и на некоторых предприятиях города Ниньбо, имеющих доступ к городской сети (Metropolitan Area Network, MAN), были установлены оконечные устройства IAD. Развертывание этого оборудования позволило

пользователям непосредственно на своем опыте проверить реализацию услуг речевой связи на основе VoIP, предоставляемых платформой Softswitch от ZTE.

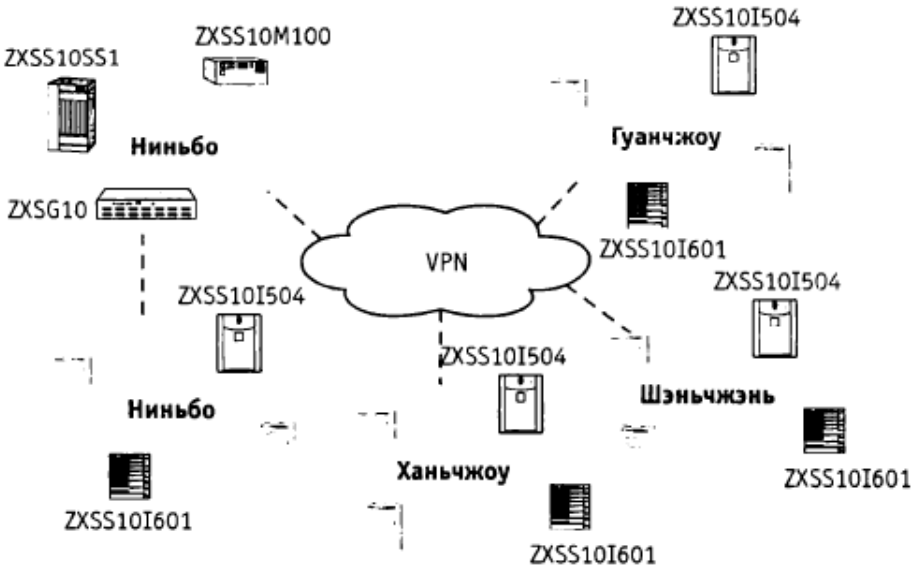


Рис. 5.18. Взаимодействие широкополосных речевых услуг, предоставляемых системой Softswitch от ZTE, в нескольких городских сетях

На третьем этапе устройства IAD были развернуты в других городах, таких как Ханьчжоу, Гуанчжоу и Шэньчжэнь. Все IAD во всех четырех городах функционируют под управлением системы Softswitch, установленной в Ниньбо, которая обеспечила возможность взаимодействия речевых услуг в пределах домена Softswitch через VoIP и взаимодействие между системой Softswitch и сетью PSTN.

Успешное развертывание сети NGN в Ниньбо подтвердило высокую надежность системы Softswitch от ZTE как системы операторского класса и как возможного решения для сети следующего поколения. Проект компании China Netcom в Ниньбо обеспечил предоставление речевых услуг, реализуемых на основе VoIP-услуги системы Softswitch от ZTE, для более чем 30 ООО абонентов.

Сетевая среда. Компания China Netcom, общая пропускная способность линий которой составляет около 40 Гбит/с, планирует создание общенациональной широкополосной телефонной сети на базе технологии Softswitch, которая позволит полностью использовать традиционные ресурсы городских сетей в каждом городе. Этот проект обеспечит обслуживание 100 ООО абонентов в 22 городах.

Для обеспечения заданного качества (QoS) речевых услуг компания China Netcom организовала VPN-сеть передачи речи, охватывающую весь Китай. VPN-сеть используется для объединения речи и данных, для того чтобы обеспечить приоритет речевой информации и облегчить управление сетью передачи речи. В речевой VPN используются частные IP-адреса. Речевое взаимодействие в сети MAN реализуется посредством внутренней маршрутизации в MAN, а речевое взаимодействие между сетями MAN обеспечивается за

счет MPLS VPN, развернутой между смежными сетями MAN. Взаимодействие на уровне передачи данных с другими MAN компании China Netcom или сетями общего пользования реализуется через NAT, подключенный к оборудованию на базовом уровне MAN посредством трансляции адресов и преобразования данных.

Организация сети. В соответствии с сетевой средой и проектными требованиями China Netcom корпорация ZTE предложила решение по локальному речевому доступу на базе Softswitch + TG + SG + IAD (включая два типа IAD с одним или несколькими интерфейсами), облегчающее реализацию пользовательского доступа и позволяющее полностью использовать сетевые ресурсы. Система состоит из базового устройства управления Softswitch, транкового шлюза, шлюза сигнализации, устройства IAD и полноценной системы управления сетью и биллинга (рис. 5.19).

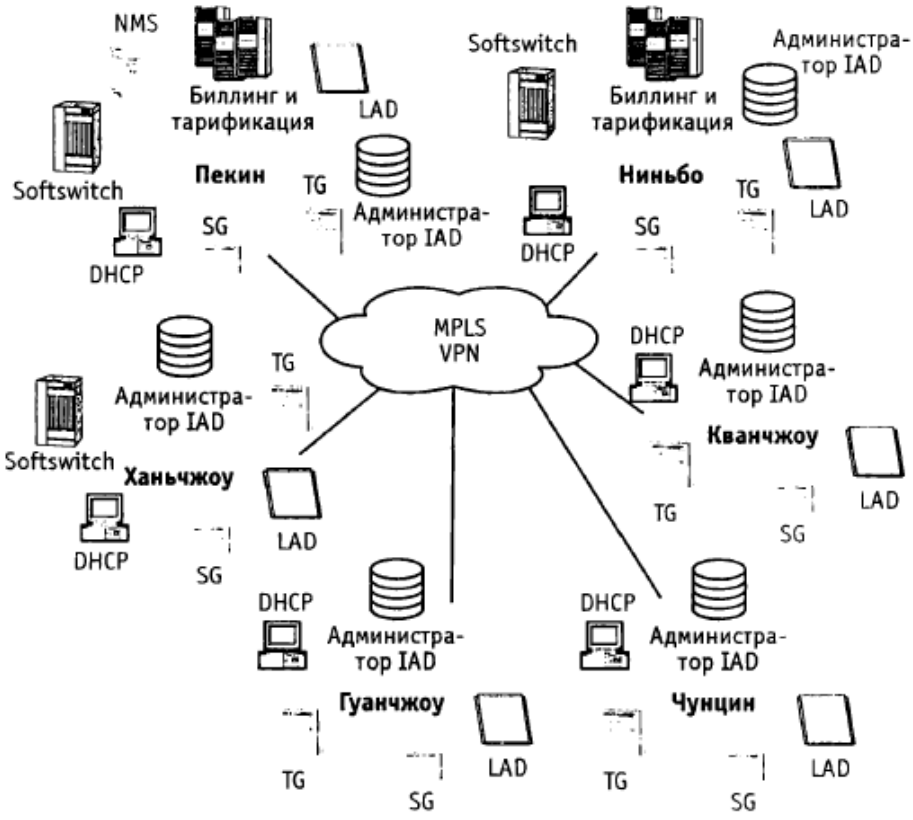


Рис. 5.19. Широкополосная телефонная сеть компании China Netcom, построенная на основе Softswitch от ZTE

На данный момент завершено строительство сети в 22 основных городах, таких как Пекин, Ханьчжоу, Ниньбо, Шанхай, Гуанчжоу и т.д., при этом базовое устройство управления ZXSS10 SS1 расположено в Пекине, и начальная проектная емкость составляет 100 000 абонентов.

4.2.2. Развертывание NGN класса 4 для China Telecom

В декабре 2001 г. корпорация ZTE со своей системой Softswitch выиграла тендер на участие в проекте построения сети следующего поколения компании China Telecom на

основе Softswitch, став, таким образом, единственным национальным поставщиком подобного оборудования. В рамках этого проекта China Telecom предполагает провести испытания технологии Softswitch и приобрести дополнительный опыт по ее использованию, а также проверить преимущества системы Softswitch и возможность ее применения в сети следующего поколения. N1GN прошла испытания в сетях пакетной коммутации компании China Telecom, при этом в качестве базовой IP-сети использовалась сеть China Netcom, а в качестве базовой сети ATM – мультимедийная широкополосная сеть общего пользования. ZTE предлагает всеобъемлющее сквозное решение для системы NGN, позволяющее проверить различные варианты ее применения, включая создание крупномасштабной сети, восстановление в аварийных ситуациях, возможность взаимодействия сетей, доступ с использованием различных терминалов, передачу изображений/видеоинформации и т.д.

В соответствии с проектом системы в городе Шэньчжень было установлено два комплекта устройства управления Softswitch ZXSS10 SS1 и два комплекта шлюзов сигнализации ZXSS10 S200. Один комплект медиа-шлюза ZXSS10 M100 был установлен в Гуанчжоу, а другой - в Шэньчжене. В качестве пользовательских терминалов в этом проекте использовались устройства IAD, SIP-телефон и PC-телефон (рис. 5.20).

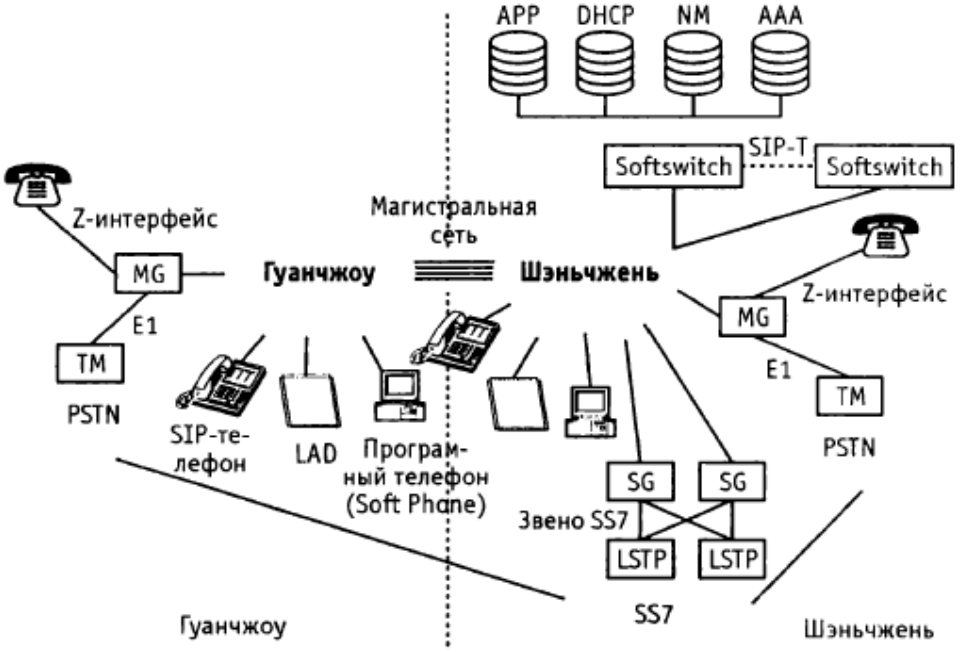


Рис. 5.20. Архитектура экспериментальной сети NGN компании China Telecom

5. КАЧЕСТВО ОБСЛУЖИВАНИЯ В IP-СЕТЯХ

Вопросы качества обслуживания (QoS) в IP-сетях в последнее время стали особенно актуальными, поскольку от их решения напрямую зависит архитектура перспективной сети связи XXI века.

За последние несколько лет в рамках организации IETF было предложено несколько архитектур и механизмов, призванных в той или иной степени обеспечить QoS. Наиболее известными и реализованными являются IntSerf, DiffSerf, MPLS (GMPLS), а также механизм принудительной маршрутизации.

5.1. Стандарты QoS ITU-T для IP-сетей

Для поддержки конвергенции IP-сетей и сетей ТфОП, IP-сети должны обеспечивать надежное дифференцированное QoS для разнообразных приложений пользователей, включая телефонию. Для обеспечения QoS из конца в конец, провайдерам IP-сетей необходимо согласовать общий набор параметров производительности передачи IP-пакетов и задачи QoS. Далее будут рассмотрены две новые рекомендации ITU-T, Y.1540 и Y.1541 по вопросам QoS.

5.1.1. Постановка вопроса

Существует широко распространенное мнение, что сегодняшние сети КК и КП постепенно объединятся в сети, основанные на IP-инфраструктуре, которая будет переносить как трафик ТфОП, так и традиционных приложений Internet. Такой сценарий конвергенции привлекателен тем, что. обеспечивает как снижение себестоимости через объединение технологий, так и развитие индустрии через создание новых услуг. Однако на практике конвергенция идет довольно медленно. С технической точки зрения главным камнем преткновения оказалась проблема качества обеспечения обслуживания (QoS). Традиционные IP-сети используют подход «наилучшей попытки» (best effort) к качеству, предоставляющий пользователям справедливую долю доступных сетевых ресурсов, но не гарантирующий выполнения никакого определенного уровня производительности. Принцип best effort был достаточно эффективен для поддержки приложений нереального масштаба времени (электронная почта, передача файлов) и был расширен для приложений, близких к реальному масштабу времени (аудио/видео вещание, просмотр Web). Основанная на текущем избытке пропускной способности многих маршрутов, парадигма наилучшей попытки сталкивается с сегодняшними потребностями многих пользователей в интерактивной голосовой телефонии и в других приложениях реального времени.

Однако маловероятно обеспечить качество, ожидаемое пользователями интерактивной голосовой телефонии и других приложений реального времени, когда ограничения пропускной способности приводят к существенному увеличению величины задержки или к потерям пакетов.

Для того чтобы реализовать полностью полезный эффект от конвергенции, будущие, основанные на IP-сети, нуждаются в использовании новых принципов разделения ресурсов, способных надежно обеспечить дифференцированное QoS для большого и многообразного набора пользовательских приложений, включающих, что особенно важно, голос поверх IP (VoIP).

Решения QoS из конца в конец для IP делают возможной успешную конвергенцию IP/ТфОП, которая может быть реализована, например, в три шага:

1. Выполнение сетевыми провайдерами соглашений относительно общего набора параметров производительности IP и требований QoS.

2. Развертывание сетевых механизмов, поддерживающих заданные требования QoS на участке терминал-терминал.

3. Внедрение требований QoS в протоколы сигнализации для возможности создания по запросу IP-потоков с гарантированным QoS.

13-я исследовательская группа Международного Союза Электросвязи (сектор стандартизации телекоммуникаций) - МСЭ-Т недавно выпустила два международных стандарта (рекомендации), которые выполняют первый из этих трех шагов. Первая рекомендация, Y.1540, определяет стандарты параметров производительности для передачи пакетов в IP-сетях. Вторая, Y.1541, специфицирует требования к стыку сетевой интерфейс-сетевой интерфейс (network-interface-tonetwork-interface, NI-NI) для параметров рекомендации Y.1540 и группирует эти численные требования по шести классам QoS для IP-сетей. Далее будет описываться развитие этих новых рекомендаций, выводы по их техническому содержанию, а также будет определено, что еще необходимо сделать для оптимизации их использования в будущих IP-сетях, гарантирующих QoS.

5.1.2. Рекомендация Y.154Q

Рекомендация Y.1540 определяет параметры, которые будут использоваться для спецификации и оценивания скорости, точности, надежности и готовности передачи IP-пакетов в международных сетях передачи данных. Параметры могут быть использованы для описания IP-потоков из конца в конец и отдельных частей сети, поддерживающих такие потоки. В соответствии с определениями Y.1540, транспорт без установления соединения является отличительной чертой IP. Y.1540 применяется к IP-потокам с использованием IP

протокола четвертой версии (IP Version 4, IPv4). Однако здесь следует отметить, что принципы и рекомендации для протокола IP шестой версии (IPv6) остаются теми же самыми.

Предполагаемые пользователи рекомендации Y.1540 - это провайдеры IP-сетей, производители оборудования и конечные пользователи. Провайдеры будут использовать Y.1540 при планировании, разработке и оценивании IP-сетей во взаимодействии с необходимой пользователям производительностью. Один крупный сетевой провайдер уже использует параметры рекомендации Y.1540 для мониторинга производительности передачи пакетов. Производители будут использовать Y.1540 при разработке и сбыте оборудования, согласующегося со спецификациями провайдера. Конечные пользователи будут применять рекомендацию для оценки производительности IP-сетей по фактическому взаимодействию между терминалами.

Процесс разработки параметров. На рис. 6.1 показан трехшаговый процесс, который традиционно использовался 13-й исследовательской группой ITU-T при разработке параметров работы цифровых сетей, и в данном же контексте установлены границы рассмотрения рекомендации Y.1540.

Первый шаг заключается в определении интерфейсов, для которых будут применяться параметры специфических событий, которые могут происходить на данных интерфейсах. Сеть моделируется как объединение сетевых сегментов, соединенных каналами передачи данных (звеньями обмена). Интерфейсы между ними, названные точками измерения (Measurement Point, MP), являются функциональными границами, на которых могут быть проведены наблюдения стандартизированных протоколов. Важные, с точки зрения работы, события, которые могут быть посчитаны, измерены во времени или сравнены в точках измерения (MP), будем называть опорными событиями (Reference Event, RE). Специфические опорные события определяются протоколом интерфейса.

Второй шаг заключается в определении набора первичных параметров, которые в совокупности характеризуют работу сети. Первичные параметры связаны с частными коммуникационными функциями и описаны в терминах опорных событий. Коммуникационная функция определяет ожидаемую реакцию сети (или сетевого сегмента) на специфическое внешнее воздействие; воздействия и реакции являются опорными событиями.

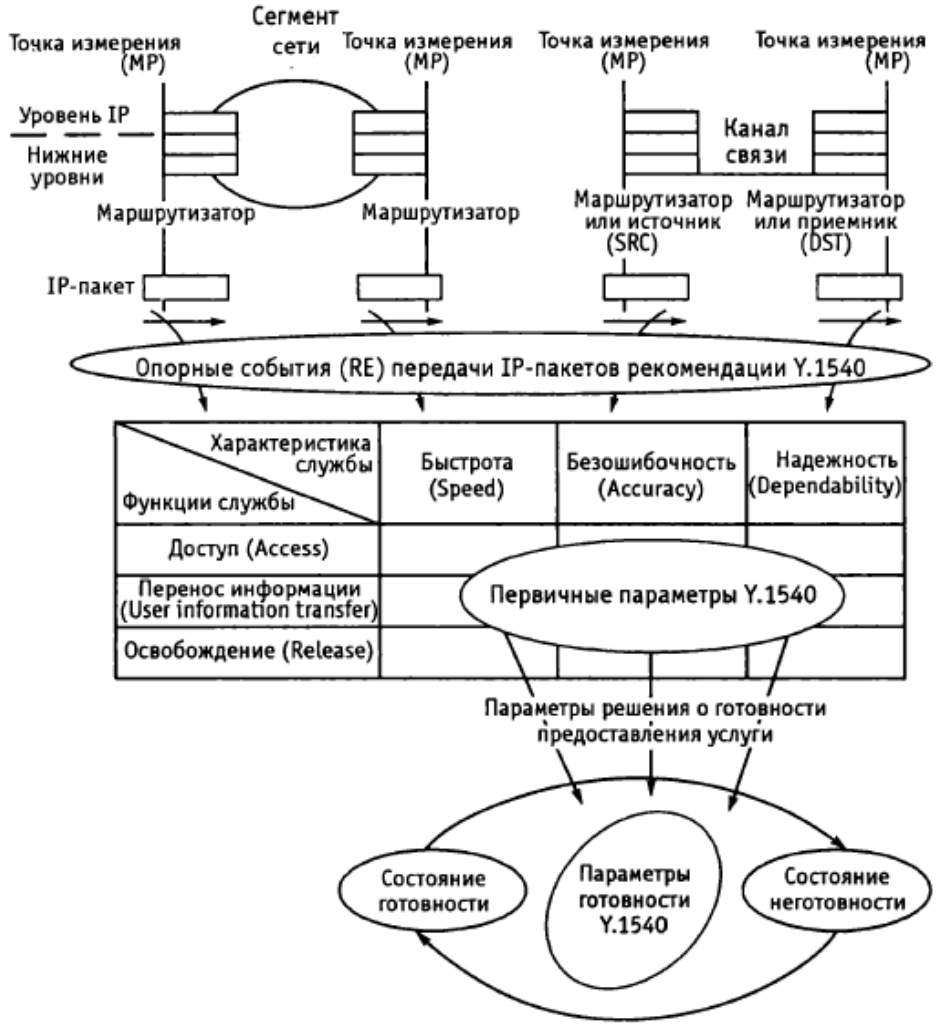


Рис. 6.1. Эталонная модель и область действия рекомендации Y.1540

При описании работы цифровой сети обычно используются три общих коммуникационных функции: доступ, передача пользовательской информации и освобождение.

Согласно статистике, параметры работы случайным образом изменяются на некотором пространстве выборок, которое различает возможные исходы, которые могут быть у функции работы. Для любой дискретной функции можно различить три общих типа исходов: успешная работа, неправильная работа и невыполнение. Соответствующие пользователю критерии работы - это: скорость, безошибочность и надежность. Они связаны с общими коммуникационными функциями в известной матрице размерностью 3x3. Для описания каждой комбинации функция/критерий в матрице определен один или несколько первичных параметров. Матричный подход помогает удостовериться, что не пропущен ни один существенный атрибут.

Третий шаг при разработке параметров заключается в определении набора параметров готовности для описания работы с более долговременной точки зрения. Параметры готовности определяются на основе наблюдаемых значений для подмножества первичных

параметров, параметров решения о готовности. Канал связи между парой (или больше) пользователей может находиться в одном из двух состояний: готовном или неготовном, что определяется функцией готовности, которая сравнивает наблюдаемые значения параметров принятия решения с соответствующими критическими порогами за последовательные периоды наблюдения. Параметры готовности характеризуют бинарный вероятностный процесс в статистических терминах.

При разработке Y.1540 13-я исследовательская группа согласилась, что точки измерений (MP) являются юридическими границами, которые разделяют независимо управляемые IP-сети (автономные системы) и пользовательские терминалы. Подходящим интерфейсным протоколом является IPv4, а подходящими информационными блоками - IP-пакеты.

Опорное событие передачи IP-пакета (IP Packet Transfer Reference Event, IPRE) для указанной пары источник/получатель (SRC/DST) происходит, когда IP-пакет с определенными IP-адресами SRC/DST (и правильной контрольной суммой заголовка) пересекает MP. Единственная коммуникационная функция, к которой обращается рекомендация Y.1540 - это передача IP-пакета (IP packet transfer), функции доступа и освобождения не рассматриваются. Это отражает тот факт, что сегодня IP-сети - это сети без установления соединения. ITU-T SG 13 и другие исследовательские группы разрабатывают параметры работы для IP-сетей, которые могли бы поддерживать такие функции в будущем (например, установление и разъединение ориентированных на соединение потоков).

Рекомендация Y.1540 определяет четыре индивидуальных результата передачи пакета, основанных на опорных событиях (RE) в точках измерений (MP), что в упрощенном виде показано на рис. 6.2. Приходящий в сегмент IP-пакет, на входящей MP может столкнуться со следующими исходами: успешная передача, ошибка или потеря.

IP-пакет, который появляется на входящей MP без соответствующей исходящей, будем называть ложным. События и результаты при передаче IP-пакета в рекомендации Y.1540 определены более формально, принимая во внимание общую информацию маршрутизации и возможность фрагментации пакетов. Различная маршрутизация объясняется определением в данное время и для данного IP-потока из конца в конец набора допустимых входящих и исходящих MP. Фрагментация пакетов объясняется определением результатов передачи пакетов когда RE на одной MP кончается несколькими соответствующими событиями на других MP. (Y.1540 также определяет результат потери мультипакетного блока и связанный с ним параметр - коэффициент потери блоков для определения и ограничения последовательных или сгруппированных (пачечных) событий потери блоков). Рабочие параметры передачи IP-пакетов. Рекомендация Y.1540 определяет пять рабочих параметров передачи IP-пакетов на основе результатов, приведенных на рис. 6.2.

Задержка передачи IP-пакета (IP Packet Transfer Delay, IPTD) – это время ($t_2 - t_1$) между возникновением двух, связанных с передачей IP пакета, событий: входящее событие RE_1 в момент времени t_1 и исходящее событие RE_2 в момент времени t_2, где ($t_2 > t_1$) и ($t_2 - t_1$) ≤ T_{max}. IPTD определен для всех удачных и ошибочных результатов передачи пакетов. Если пакет фрагментирован, то t_2 - это время соответствующего последнего выходного события. Подразумевается, что задержка передачи IP-пакета, специфицированная в рекомендации Y.1541 - это среднее арифметическое задержек IP-пакетов.

Джиттер задержки IP-пакетов (IP Packet Delay Variation, IPDV) определяется на основе наблюдений соответствующих потоков IP-пакетов на входящих и исходящих MPs (например, MP_1 и MP_2 на рис. 6.13). Джиттер задержки пакетов (v_k) для IP-пакета к между MP_1 и MP_2 - это разность между абсолютной задержкой (x_k) передачи IP-пакета и определенной задержкой ($d_{1,2}$) передачи контрольного IP-пакета между этими самыми MPs: $v_k = x_k - d_{1,2}$. Задержка передачи контрольного IP-пакета $d_{1,2}$ между SRC и DST - это абсолютная задержка передачи IP-пакета, определяемая первым IP-пакетом между этими двумя MPs. (Положительные значения IPDV соответствуют большим задержкам пакета, чем определенные контрольным пакетом, а отрицательные значения - соответственно меньшим. Распределение !PDV идентично распределению абсолютных задержек передачи пакетов, сдвинутых на постоянную величину $d_{1,2}$).

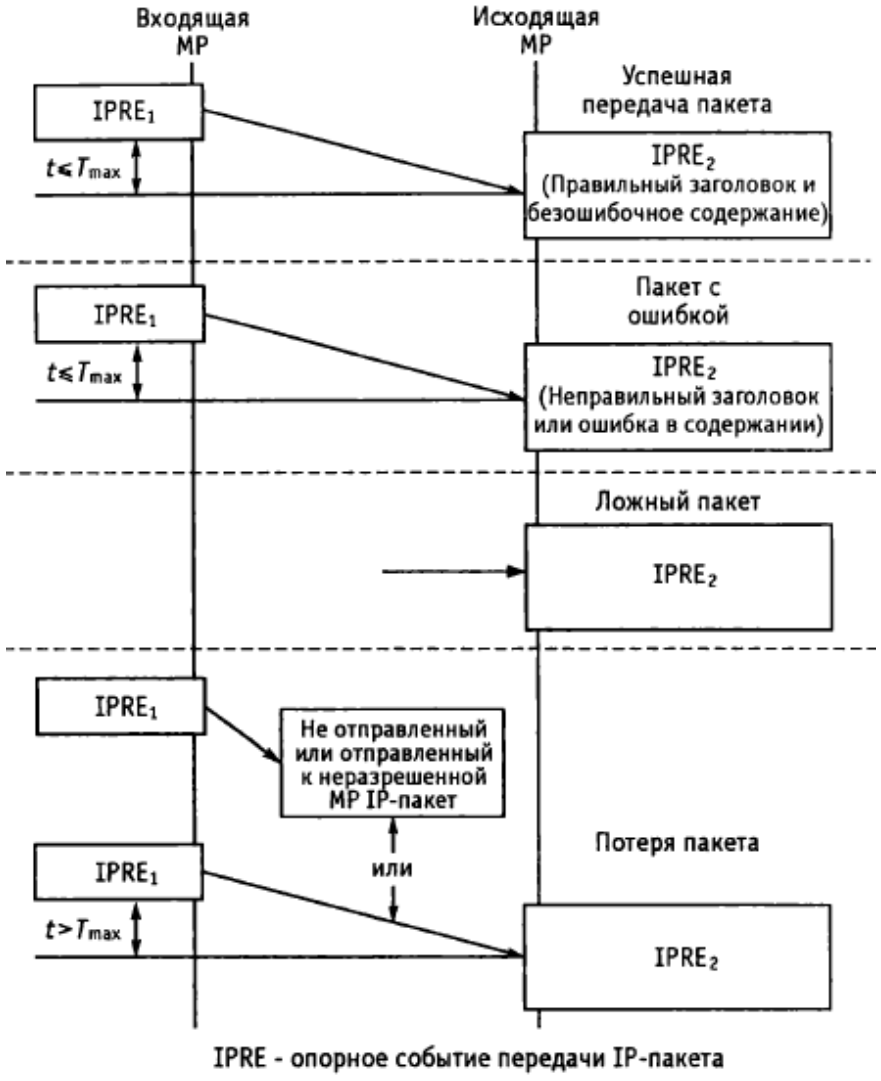


Рис. 6.2. Возможные исходы передачи IP-пакета

Коэффициент потери IP-пакетов (IP Packet Loss Ratio, IPLR) – это отношение общего числа потерянных пакетов к общему числу переданных пакетов в общей совокупности.

Уровень ложных пакетов (Spurious IP packet rate, SIPR) на исходящей МР - это общее число ложных пакетов, наблюдаемых на исходящей МР в течение определенного интервала времени, ограниченного длительностью этого интервала (например, число ложных пакетов в секунду). Этот параметр выражен как уровень за определенное время, а не как отношение, поскольку механизмы, причиной которых является появление ложных пакетов, имеют мало общего с числом переданных IP-пакетов.

Хотя и не исчерпывающе, эти параметры вместе описывают основные рабочие отношения пользователей IP сетей. Задержка передачи IP-пакета описывает среднее время, затрачиваемое сетью на передачу пакета между входящей и исходящей МР. Ограничения IPTD будут решающими для успешного развертывания VoIP, видеоконференцсвязи и приложений реального времени и будут оказывать сильное влияние на принятие клиентами других услуг. Изменение задержки пакетов характеризует джиттер во времени опорных

событий передачи пакета на исходящем интерфейсе по отношению к соответствующей модели входных событий. IPDV должен контролироваться для избежания недогрузки или перегрузки IP-маршрутизаторов или буферов терминалов. Коэффициент потери IP-пакетов выражает вероятность того, что пакет, вверенный сети на входном интерфейсе, не доставлен соответствующей выходной точке (точкам).

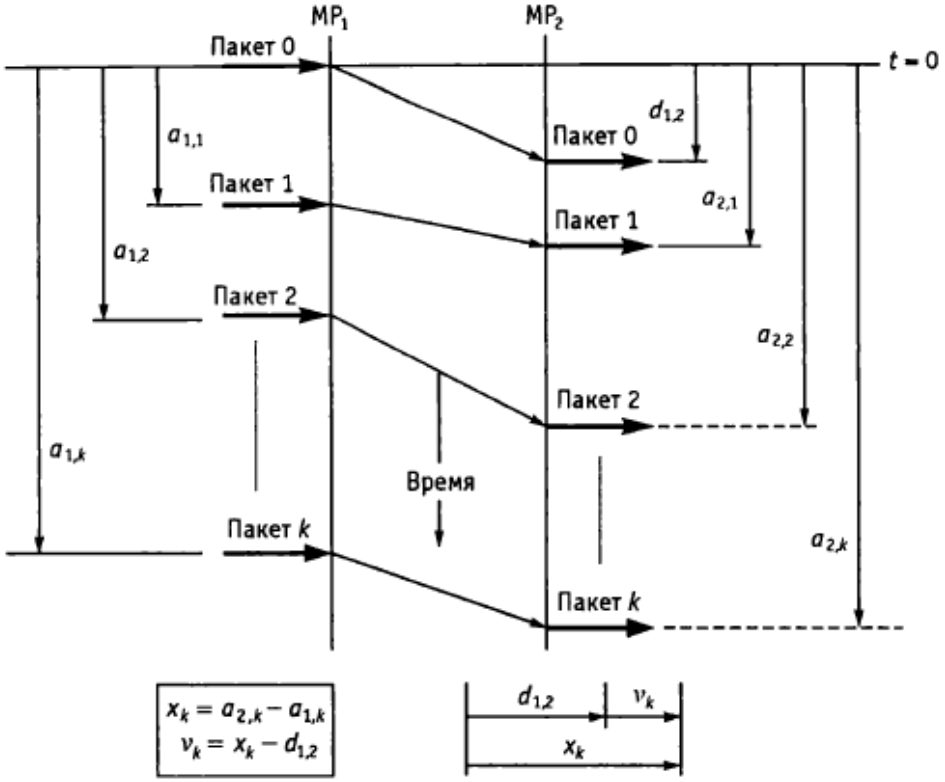


Рис. 6.3. Джиттер задержки IP-пакетов

Коэффициент IPLR должен ограничиваться для гарантирования разборчивости и приемлемого качества изображения для голосовых и видеоприложений реального времени, а также обеспечения приемлемого качества других приложений. (Учет последовательной потери пакетов представляет особый интерес для некоторых неэластичных приложений реального времени, таких как голос и видео. Коэффициент потери блоков - один из путей для характеристики таких событий). Коэффициент ошибок IP-пакетов и уровень ложных пакетов выражают вероятность, что данные пользователя на выходном интерфейсе отличаются от входных данных в результате искажения, дублирования или неправильной маршрутизации в сети.

В нормативном наборе рекомендаций Y.1540 отсутствуют любые параметры, которые описывают скорость передачи данных пользователя или пропускную способность, обеспечиваемую сегментом сети. Y.1541 обращает внимание на то, что производительность и другие связанные с потоками вопросы рассматриваются, используя дескриптор трафика IP-

сети, определенный в сопутствующей рекомендации Y.1221. База для возможной будущей работы по определению метрик большой пропускной способности представлена в RFC 3148.

Параметры готовности. Как определено в Y.1540, готовность относится к однонаправленному IP-потоку между определенной парой (или набором) МР. В Y.1540 функция готовности определяет IPLR как единственный параметр принятия решения о доступности. Для данного потока сетевой сегмент определяется как готовный на отрезке наблюдения, если наблюдаемое значение IPLR для потока ниже порога c_1. Иначе сегмент не готовен. Y.1540 определяет значение c_1 равное 0,75 и отмечает, что спецификации ожидаемого значения IPLR должны исключать все периоды неготовности (т. е. все интервалы времени, в течение которых наблюдаемое значение IPLR превышает Ст). Рекомендация определяет минимальный период наблюдения готовности в 5 мин. (Мониторинг низкоуровневой работы и ошибок сетевых элементов может разрешить идентификацию надвигающейся неготовности в более короткое время и направить корректирующее действие.) Определение готовности предназначено для использования в работе характеризуемой сети как для нормального трафика между источником и получателем, так и для синтетического трафика, генерируемого наборами тестов или другими устройствами измерения. Y.1540 отмечает, что испытательный трафик должен быть ограничен так, чтобы это не вызывало перегрузок, которые могут исказить результаты испытаний.

Рекомендация Y.1540 определяет два рабочих параметра готовности. Для данного сетевого сегмента и потока процент готовности – это доля от запланированного времени готовности, в течение которого сегмент фактически поддерживает поток в готовном состоянии. Процент неготовности - это дополнение предыдущего параметра, т. е. доля от запланированного времени готовности, в течение которого поток является неготовным.

При любом задании сумма двух значений равна 100 %. Базовый период для планирования времени готовности ограничен, чтобы исключить любые согласованные периоды неготовности (например, запланированное время простоя для профилактического техобслуживания).

5.1.3. Рекомендация Y.1541

Рекомендация ITU-T Y.1541 определяет числовые значения, которые должны быть достигнуты на международных отрезках IP-сетей между оконечными терминалами пользователей для каждого из ключевых параметров работы, определенных в рекомендации Y.1540. Указанные значения сгруппированы в некоторое число различных классов QoS для установления практической базы для связи между конечными пользователями и провайдерами сетей, а также и среди провайдеров по качеству, которое будет

поддерживаться из конца в конец на отрезках IP-сетей. С одной стороны, операторы сетей признают, что работа из конца в конец ограничивается самым плохо работающим сегментом сети, и требования пользовательских приложений могут быть удовлетворены только, если каждая из объединенных сетей разработана и функционирует с учетом этих требований. С другой стороны, операторы знают, что наличие рабочих спецификаций дает ощутимый толчок сетевой экономике, играя роль в дифференциации конкурентоспособного продукта и маркетинге, и если оператор берет на себя определенные обязательства, то пользователи ожидают их выполнения. То что эти переговоры регулярно следуют, позволяет, несмотря на технологическое разнообразие независимо управляемых сетей, сотрудничать в обеспечении надежной, высококачественной всемирной связи. При определении характеристик работы из конца в конец для конкретных пользовательских приложений и сетевых технологий, 13-я исследовательская группа ITU-T применила два исторически сложившихся, дополняющих друг друга и конкурирующих подхода для оценки работы. Первый «нисходящий» метод переводит требования приложения пользователя и ожидаемое качество в числовые значения стандартизированных ITU-T параметров, что наблюдается в интерфейсах пользователь/сеть. Такой нисходящий перевод сделан для каждой широкой категории пользовательских приложений и должен обеспечить изменчивость в функциональности терминала и работе. Второй «восходящий» метод переводит технические спецификации, определяющие возможности и ограничения отдельных сетевых элементов в числовые значения тех же самых, стандартизированных ITU-T параметров работы, наблюдаемых в тех же самых интерфейсах пользователь/сеть. Восходящий перевод основан на базовых конфигурациях, идентифицирующих типичные связи сетевых путей (линий) и узлов, и наихудших значенях ключевых переменных типа географических расстояний между сетевыми интерфейсами. В разделенных сетях также должны рассматриваться и другие переменные, такие как пропускная способность сети, предполагаемый трафик и механизмы управления ресурсами. В идеале, восходящий и нисходящий методы производят наложение диапазонов значений для стандартизированных параметров, из которых одна или более характеристика может быть специфицирована.

Процесс выбора числовых характеристик работы был особенно трудоемким в случае рекомендации У.1541. По нисходящей перспективе ключевой проблемой было охватить разнообразнейший набор пользовательских приложений и терминалов. Участники 13-й исследовательской группы были в состоянии ограничить и сегментировать пространство приложений, систематически рассматривая для каждого приложения функциональные отношения между удовлетворением пользователя и значениями параметров рекомендации У.1541. Нисходящий анализ был значительно облегчен близкой связью с 12-й

исследовательской группой, которая уже много лет специализировалась по вопросам воспринимаемости качества и принятия конечным пользователем определенных приложений и медиа (например, речь, изображение, текст) при ухудшении сетевой передачи, принимая во внимание работу телефонного, аудиовизуального и интерактивного голосового терминалов.

13-я исследовательская группа получила серьезную поддержку в виде информации относительно восходящего подхода от сетевых провайдеров по характеристикам возможностей работы, ограничениям доступных сетевых элементов и определению реалистичных базовых конфигураций.

Восходящий и нисходящий анализы быстро подтвердили, что не существует единственного набора уровней работы IP-сети, который мог бы экономно поддерживать все предполагаемые приложения для будущих, основанных на IP-инфраструктуре сетей; соответственно, 13-я исследовательская группа взяла на себя ответственность по определению нескольких наборов характеристик работы - классов OoS рекомендации Y.1541.

Выбор классов OoS, которые должны были быть включены в Y.1541, обсуждался на 4-й рабочей встрече 13-й исследовательской группы на протяжении нескольких заседаний. В ранних дискуссиях участники рассматривали подход, касающийся каждого параметра, который позволял бы пользователям определять значения для каждого параметра независимо. Однако все довольно быстро согласились, что разрешение подобной свободы выбора будет слишком сложно осуществить. Фактически имелось четкое согласие, что число различных классов QoS, специфицированных в Y.1541, должно быть строго ограничено, чтобы избежать чрезмерного усложнения рекомендации (и, что более важно, сетевых технологий, требуемых для реализации этого). Для обеспечения наибольшего охвата группа согласилась, что определенные классы должны все вместе охватить широкий набор приложений и высокий процент нужд пользователей на отсталых IP-сетях. В дополнение к традиционным приложениям Интернет сюда же включены телефония точка-точка, мультимедийные телеконференции и интерактивная передача данных (например, сигнализации). Группа заключила, что потребности некоторых, особо требовательных приложений (например, видео реального времени высокого разрешения, широкополосные TCP соединения) пока не будут отражены в стандартных классах. Было согласовано, что каждый класс QoS должен охватывать группу приложений с подобными требованиями работы, значительно отличающимися от требований других классов. И здесь, с точки зрения ограничения сложности структуры классов, может быть задан вопрос, будут ли операторы управляемых IP-сетей для каждой пары предложенных классов делать какие-нибудь

различия при их осуществлении. Классы QoS будут различаться только при утвердительном ответе на этот вопрос.

Эталонный маршрут рекомендации Y.1541. Характеристики работы IP из конца в конец, определенные в рекомендации Y.1541, применяются от NI до NI, как показано на рис. 6.4. Сетевой маршрут из конца в конец в IP-сети включает набор сетевых сегментов и каналов передачи, транспортирующих IP-пакеты от SRC до DST. Нижние протоколы, включающие уровень IP вместе с SRC и DST, могут также рассматриваться как часть IP-сети. Сетевые сегменты соответствуют областям операторов и могут содержать архитектуры доступа к IP-сети. Устройство клиента включает в себя все терминальное оборудование, такое как хосты, и любые оконечные маршрутизаторы или ЛВС.

Характеристики и классы QoS. Характеристики работы и классы QoS рекомендации Y.1541 представлены в табл. 6.1. Каждый класс QoS создает определенную комбинацию границ на подмножестве значений рабочих характеристик. Классы и связанные с ними характеристики работы применяются к потокам IP-пакетов между MP, которые разграничивают IP сеть из конца в конец (т.е. сетевые интерфейсы (СИ), показанные на рис. 6.4). Поток IP-пакетов - это трафик, ассоциированный с данным соединением или потоком без установления соединения, имеющим те же самые хост источника (SRC), хост назначения (DST), класс обслуживания и идентификацию сессии. Другие документы могут использовать термины «микропоток» и «подпоток» в отношении потоков трафика при такой степени классификации.

Классы 0 и 1 определяют верхние границы по задержке передачи пакетов и потерям пакетов. Они также ограничивают джиттер задержки. Классы 2 и 3 определяют верхние границы по задержке передачи пакетов и потерям пакетов, но не ограничивают джиттер задержки. Классы 0 и 2 отличаются от классов 1 и 3 по характеристикам передачи пакетов. Класс 4 ограничивает потери пакетов и обеспечивает довольно «мягкую» верхнюю границу задержки. Y.1541 также определяет неспецифицируемый класс (класс 5), не предоставляющий никаких определенных гарантий работы. Значение для характеристики потери одиночных пакетов было выбрано для того, чтобы гарантировать, что потеря пакета - доминирующая причина дефектов, представленных верхними уровнями. Характеристики QoS применимы, когда скорость каналов доступа соответствует скоростям T1 или E1 или выше. Характеристики IPTD классов 0 и 2 будут не всегда достижимы на длинных маршрутах. Y.1541 предполагает, что пользователь и провайдер сети должны согласовывать профиль трафика, который применяется к одному или более потокам пакетов по классу QoS. В настоящее время соглашающиеся стороны могут использовать любые спецификации пропускной способности, которые они считают приемлемыми, до тех пор, пока они

осуществимы и проверяемы. Например, пиковая скорость передачи в битах (включая издержки нижних уровней) может быть достаточной. Когда доступны протоколы и системы, поддерживающие динамические запросы, пользователи могут заключать соглашение о трафике, определяющее один или несколько параметров трафика в соответствии с рекомендацией Y. 1221.

Таблица 6.1. **Определение классов QoS и характеристик IP-сети**

Параметр работы сети	Суть рабочей характеристики	Классы QoS					
		класс 0	класс 1	класс 2	класс 3	класс 4	класс 5
IPTD	Предельное значение среднего значения IPTD, мс	100	400	100	400	1000	Н
IPDV	Предельное значение, мс	50	50	Н	Н	Н	Н
IPLR	Предельное значение вероятности потери пакета	$1\cdot10^{-3}$	$1\cdot10^{-3}$	$1\cdot10^{-3}$	$1\cdot10^{-3}$	$1\cdot10^{-3}$	Н
IPER	Предельное значение	$1\cdot10^{-4}$	$1\cdot10^{-4}$	$1\cdot10^{-4}$	$1\cdot10^{-4}$	$1\cdot10^{-4}$	Н

Н – неспецифицировано

Сети, предлагающие 1P-коммуникации в соответствии с У.1541, как ожидается, будут поддерживать эти границы (пределы) из конца в конец для времени существования потока до тех пор, пока пользователи (и другие сети) не превысят согласованную пропускную способность. Рекомендация предусматривает, что сети, выполняющие Y.1541, не обязаны поддерживать согласованные значения QoS при превышении установленной пропускной способности. Сеть, испытывающая такой избыточный поток, может отбрасывать число пакетов, равное числу пакетов превышения. Такие отброшенные пакеты не учитываются как потерянные при оценке параметра IPLR работы сети.

Таблица 6.2. **Руководство по классам QoS для IP**

Класс QoS	Приложения (примеры)	Узловые механизмы	Сетевые технологии
0	Реального времени, чувствительные к джиттеру, с высокой интенсивностью обмена данными (VoIP, видео телеконференции)	Раздельные очереди с предпочтениями обслуживания, отвод трафика	Принудительная маршрутизация и размещение
1	Реального времени, чувствительные к джиттеру, интерактивные (VoIP, видео-телеконференции)		Менее принудительная маршрутизация и размещение
2	Транзакции, высокая интерактивность (например, сигнализации)	Раздельные очереди, приоритеты потерь	Принудительная маршрутизация и размещение
3	Транзакции, интерактивность		Менее принудительная маршрутизация и размещение
4	Только низкие потери (короткие транзакции, блоки данных, потоковое видеовещание)	Длинные очереди, приоритеты потерь	Любой маршрут/ путь
5	Традиционные приложения существующих IP-сетей	Раздельные очереди (низший приоритет)	Любой маршрут/ путь

В дополнение к характеристикам работы и классам QoS рекомендация Y.1541 определяет различные вспомогательные переменные (минимальные периоды наблюдения, длину тестовых пакетов, типовые размеры и т.д.) для облегчения оценки работы и сравнения. Например, минимальный интервал наблюдения в 10...20 секунд рекомендуется для оценки VoIP при типовой скорости передачи пакетов (50-100 пакетов в секунду). Рекомендуемый интервал наблюдения за потерями, задержками и IPDV равняется 1 мин, соблюдая баланс между статистической достоверностью и значимостью для работы пользователя. Табл. 6.2 представляет собой руководство по применению и разработке классов QoS. Y.1541 отмечает, что эти руководящие принципы являются полностью предоставленными на собственное усмотрение; провайдеры сетей могут использовать любые выбранные ими механизмы узлов, ограничения маршрутизации или другие технологии.

5.1.4. Заключение и направление будущих работ

Рекомендации ITU-T Y.1540 и Y.1541 совместно обеспечивают ключевое решение головоломки QoS в IP. Y.1540 определяет стандартные рабочие параметры передачи пакетов в IP-сетях. Y.1541 устанавливает характеристики NI-NI для параметров Y.1540 и группирует эти численные характеристики по шести отдельным классам QoS для IP-сети.

Весь набор классов охватывает главные категории IP-приложений пользователя. Рабочие значения специфицируемых параметров могут быть достигнуты в реальных сетях и могут быть проверены в подведомственных границах, оборудованных терминальным оборудованием или межсетевыми функциями. Эти рекомендации документируют важное соглашение между сетевыми провайдерами, производителями оборудования и конечными пользователями по уровням качества, которые должны поддерживаться для широкого диапазона IP-приложений, включая телефонию. Они же могут использоваться как база для установления соглашений между сетями, а также для поддержания взаимодействия по QoS среди различных технологий.

Хотя Y. 1540/Y. 1541 представляют собой полезный шаг вперед, успешное развитие, основанных на IP сетей следующего поколения, обеспечивающих динамический набор определенных классов QoS, не поддерживается. Сегодня механизмы QoS еще не являются широко распространенными на IP-сетях.

Хотя соглашения о статичных классах QoS могут осуществляться и сегодня путем сопоставления маркировки пакета (например, поля TOS или DiffServ code points) с определенным классом QoS, все еще необходима работа по определению более гибкой архитектуры QoS и установлению того, как применять классы QoS рекомендации Y.1541 в протоколах сигнализации.

Провайдерам необходимо будет определять и, возможно, стандартизировать средства распределения рабочих характеристик среди нескольких независимых сетей, которые будут типично взаимодействовать в предоставлении IP-потоков с гарантированным QoS между конечными терминалами пользователей. Говоря короче, продолжающаяся конвергенция IP/ТфОП потребует слияния мысли и действия в отношении QoS IP-сетей. 13-я исследовательская группа ITU-T и другие организации по стандартизации работают над этой задачей.

5.2. Стратегии сосуществования IPv6 и IPv4 в сетях следующего поколения

Версия 6 протокола IP. IPv6, шестая версия межсетевого протокола IP, разрабатывается для того, чтобы преодолеть следующие ограничения версии IPv4 (четвертой, используемой ныне в Интернет):

- Пространства 32-битных адресов уже не хватает.
- IPv4 плохо управляет качеством предоставляемых услуг.
- IPv4 не имеет встроенных средств защиты.

В IPv6 предусмотрены 128-битные адреса, что представляется вполне достаточным.

Заголовок пакета IPv6 состоит из стандартного 40-байтного заголовка, за которым могут следовать дополнительные заголовки. Стандартный заголовок имеет следующий формат:

[Version | Priority | Flow | Tota I Length | Next Header | Hop Limit| SA | DA]

В поле Flow указывается ожидаемое качество обслуживания пакета и, возможно, характеристики соединения, которому принадлежит пакет. Маршрутизатор может использовать это поле для управления ресурсами данного соединения и назначения пакетов для передачи. Поле Hop Limit имеет то же значение, что и поле Time to live в IPv4. Поле Next Header указывает на протокол транспортного уровня (например, TCP или UDP), если больше нет дополнительных заголовков, или на следующий дополнительный заголовок. Было определено шесть дополнительных заголовков:

- Hop-by-Hop: используется маршрутизаторами для предоставления информации о доставке пакетов.
- Destination: определяет опции, согласованные с оконечной системой.
- Routing: задает предпочтительный путь в тех случаях, когда маршрутизация определяется отправителем.
- Fragmentation: для фрагментации больших дейтаграмм.
- Authentication: определяет правила аутентификации.
- Encryptedpayloach содержит шифрованную полезную информацию.

Каждый дополнительный заголовок содержит поле Next Header, указывающее на протокол транспортного уровня, если нет других дополнительных заголовков, или на следующий дополнительный заголовок.

Обычно фрагментирует пакеты в IPv6 сам компьютер-источник, а не промежуточные маршрутизаторы. Для осуществления фрагментации хост-отправитель должен определить максимальную длину блока на пути до получателя. Маршрутизаторы IPv6 реализуют алгоритм для вычисления пути МДБ. Хост-отправитель всегда может отправить сообщение через определенный маршрутизатор или через поставщика услуг P при помощи туннеля (осуществляющего инкапсуляцию в пакеты для P) или с помощью дополнительного заголовка Routing.

IPv6 использует для маршрутизации протокол IDRP (Interdomain Routing Protocol, междоменный протокол маршрутизации), основанный на алгоритме предпочтительного пути, более мощный, чем BGP; протокол IDRP может работать с несколькими семействами адресов, такими, например, как адреса IPv4 и IPv6.

IPv6 был разработан, помимо прочего, для расширения адресного пространства, чтобы удовлетворять будущие требования работы сетей. В данном разделе будут проанализированы и обсуждены важные аспекты сценариев развертывания IPv6 и предложена системная архитектура, совместимая и интегрируемая с сетями IPv4/MPLS, а также исследованы различные стратегии развертывания IPv6 с приведением примеров проектирования сетей. Затем будет предложено развертывание IPv6 на оборудовании поставщиков услуг.

Непрерывный рост глобальной сети Интернет требует развития архитектуры сетей для приспособления к новым технологиям, что в свою очередь необходимо для поддержки растущего числа пользователей, приложений, устройств и услуг. IPv6 разработан для удовлетворения этих требований и позволяет возвратиться к глобальной сквозной среде, где сетевые правила адресации становятся прозрачными для приложений. Текущее адресное пространство IP не способно удовлетворить огромный рост числа пользователей или географические потребности расширения Интернет, не говоря уже о требованиях вновь появляющихся приложений, таких как персональный карманный компьютер (Personal Digital Assistant, PDA), домашние сети (Home Area Network, HAN), транспортировка с помощью Интернет-соединений, интегрированные телефонные услуги и распределенные игры. IPv6 увеличивает в 4 раза число битов сетевого адреса с 32 бит (в IPv4) до 128 бит, что дает более чем достаточное число уникальных глобальных IP-адресов для каждого сетевого устройства на планете. Использование уникальных глобальных IP-адресов упрощает механизмы, используемые для достижения доступности и сквозной безопасности сетевых устройств,

функционально критичных для управления приложениями и услугами, зависящими от адресов. Срок службы IPv4 был продлен использованием методов, таких как повторное использование адресов с трансляцией и лимиты временного использования. Хотя эти методы, как может показаться, увеличивают адресное пространство и соответствуют традиционной схеме клиент/сервер, они не в состоянии удовлетворить требования новых приложений. Потребность в постоянно работающем оборудовании (например, резидентский домашний Интернет через широкополосный кабельный модем или Ethernet) препятствует методам преобразования, объединения и временного использования IP-адресов. Причем требуемый «plug-and-play» для устройств пользователей Internet еще больше увеличивают требования к адресу. Гибкость адресного пространства IPv6 обеспечивает поддержку частных адресов, но должна ограничить использование технологии трансляции сетевых адресов (Network Address Translation, NAT) по причине широкой доступности глобальных адресов. IPv6 повторно предоставляет сквозную безопасность, что не всегда возможно через основанные на NAT сети.

В данный момент мы находимся на ранней стадии внедрения IPv6 с малым числом приложений IPv6 по сравнению с IPv4 на рынке и малым числом сетевых продуктов, нуждающихся в обмене между доступными услугами IPv6. Хотя, в конечном счете, успех IPv6 будет зависеть от инновационных приложений, работающих по IPv6, ключевая часть разработки IPv6 - это его способность интеграции и совместного использования с уже существующими IP-сетями. Предполагается, что хосты (узлы) IPv4 и IPv6 будут вынуждены сосуществовать довольно продолжительное время неуклонного перехода от IPv4 к IPv6, и как раз разработка переходных стратегий, инструментов и механизмов и была основной частью проекта IPv6 с самого начала. Выбор стратегии (или стратегий) внедрения будет зависеть от текущего состояния сетевой среды и таких факторов, как прогнозируемый объем трафика IPv6, доступность приложений IPv6 для конечных систем и стадии развертывания. Мы сделаем попытку подвести итог различным стратегиям интеграции/совместного использования IPv6 вместе с примерами проектов сетей, а также предложим системную архитектуру, интегрирующуюся и совместно используемую с сетями IPv4/MPLS. Будет кратко обсужден проект сети IPv6 для сетевой среды поставщика услуг со сравнением стратегий развертывания.

5.2.1. Стратегии интеграции и сосуществования IPv6 и IPv4

Успешное утверждение на рынке любой новой технологии зависит от простоты ее интеграции с существующей инфраструктурой без существенного разрушения услуг. В определении стратегий внедрения IPv6 принимали участие несколько рабочих групп IETF

(Internet Engineering Task Force), например рабочие группы IPv6, v6ops. Ниже будут рассмотрены следующие сценарии развертывания:

- магистраль двойного стека;
- IPv6 по туннелям IPv4;
- механизмы трансляции протоколов;
- выделенные каналы данных;
- магистрали MPLS.

Далее будут кратко пересмотрены и сравнены первые три сценария развертывания, а также предложены и обсуждены сценарии IPv6 по выделенным каналам данных и магистрали MPLS.

Краткий обзор механизма перехода. Сосредотачиваясь на первичной цели обеспечения взаимодействия приложений IPv6 на хостах, многие сетевые разработчики рекомендуют сначала развертывать IPv6 на периферии, где находятся приложения и хосты, а затем постепенно двигаться к ядру сети, для того чтобы снизить издержки, неустойчивость работы и воздействие интеграции. К тому же, перемещение IPv6 на периферию (в расположение пользователя) является относительно более легким, поскольку основные операционные системы (например Microsoft, Linux) уже поддерживают IPv6.

Ключевые стратегии развертывания IPv6 на периферии сети включают перенос трафика IPv6 по инфраструктуре сети IPv4, позволяя изолированным доменам IPv6 связываться друг с другом до тех пор, пока не будет осуществлен полный переход к магистралям IPv6. Затем, когда настанет время планирования полной модернизации, будет возможно перемещать через сеть и IPv6 и IPv4 с любой периферии через ядро. Дополнительно может потребоваться механизм трансляции для работы устройств, поддерживающих только IPv6 или IPv4, для того чтобы хосты, поддерживающие только один протокол, могли прозрачно связываться с хостами, работающими по другому протоколу. Все методы предполагают модернизацию сетей и постепенное развертывание IPv6 без или с небольшим разрушением услуг IPv4.

Ниже рассмотрены четыре ключевых метода развертывания IPv6.

Внедрение на магистрали двойного стека. Этот метод позволяет приложениям IPv4 и IPv6 совместно работать на магистрали с двойной маршрутизацией IP-уровня. Все маршрутизаторы (например, оборудование доступа клиента, мультиплексирующие или магистральные маршрутизаторы) в сети должны быть модернизированы до двухстековых для соединений IPv4, используя стек IPv4, а для соединений IPV6 - соответственно стек IPv6. Протоколы маршрутизации для обеих версий IP должны быть выбраны и адекватно сконфигурированы. Внутренний протокол шлюза (Interior Gateway Protocol, IGP) - это выбор между решением «корабль в ночи» (например, OSPFv2 для IPv4 и 0SPFv3 для IPv6) и

интегрированным решением (например, ISIS), обеспечивая выравнивание топологий IPv4 и IPv6.

Внедрение IPv6 по туннелям IPv4. Эти туннели инкапсулируют трафик IPv6 в пакеты IPv4, что применяется, прежде всего, для связи между изолированными областями IPv6 или для соединений с удаленными сетями IPv6 через магистраль IPv4. Технология предполагает использование вручную сконфигурированных туннелей, туннелей общей маршурутированной инкапсуляции (Generic Routing Encapsulation, GRE), полуавтоматических механизмов туннелирования, таких как услуги туннельного брокера, и полностью автоматических механизмов туннелирования, таких как 6в4 (6to4), для глобальной сети и протокола автоматической адресации туннелей внутренних областей (Intrasite Automatic Tunnel Addressing Protocol, ISATAP) для сетей кампусов. Это достаточно легкий сценарий для внедрения с технологии IPv6.

Внедрение IPv6 с использованием выделенных каналов передачи данных. Данная технология позволяет обеспечить связь между доменами IPv6 используя тот же самый второй уровень инфраструктуры, что используется для IPv4, но с использованием для IPv6 технологии Frame Relay или асинхронного режима передачи (Asynchronous Transfer Mode, ATM), постоянных виртуальных каналов (Permanent Virtual Circuit, PVC), разделенных оптических линий или разных длин волн в технологии плотного мультиплексирования по длине волны (Dense Walelength Division Multiplexing, DWDM).

Внедрение IPv6 на магистралях MPLS. Данная технология позволяет доменам IPv6 взаимодействовать друг с другом поверх магистрали IPv4/MPLS без модификации структуры ядра. В различных точках сети доступны различные технологии, но каждая требует некоторых изменений магистральной инфраструктуры или изменения конфигурации маршрутизаторов ядра, потому что пересылка основа на на метках, а не на самих заголовках IP-пакетов.

После краткого описания стратегий развертывания IPv6 приведем более подробное.

Внедрение двойного стека IPv4/IPv6. Магистраль двойного стека является основной стратегией для маршрутизации обоих протоколов- IPv4 и IPv6. Приложения, не модернизированные для поддержки стека IPv6, могут совместно работать с модернизированными приложениями в одной и той же конечной системе. Для поддержки адресов IPv4 и IPv6 и запросов службы доменных имен (Domain Name Service, DNS) был определен новый прикладной программный интерфейс (Application Programming Interface, API). Приложения выбирают между использованием IPv4 или IPv6, основываясь на поиске имени; оба адреса и IPv4 и IPv6 могут быть возвращены DNS с требованием (или согласно

системе, соответствующей правилам, определенным в документе IETF «Ошибка выбора адреса для IPv6») выбора правильного адреса на основании типа IP-трафика.

При развертывании магистрали двойного стека, все маршрутизаторы сети должны быть модернизированы до двухстековых. Сегодня, маршрутизация с использованием двойного стека протоколов – это вполне обоснованная стратегия для специфических сетевых инфраструктур со смешанным использованием IPv4 и IPv6 (например, на кампусе или агрегированной точке присутствия), требующих конфигурации обоих протоколов. Однако, кроме очевидной необходимости модернизации всех маршрутизаторов сети, менеджеры сети, выбирающие этот подход, должны знать, что все маршрутизаторы в данном случае потребуют определения двойной схемы адресации, потребуют двойного управления протоколами маршрутизации и должны будут быть сконфигурированы с достаточным объемом памяти для обеих маршрутных таблиц - для IPv4 и IPv6.

Внедрение IPv6 по туннелям IPv4. Туннелирование - это одна из ключевых стратегий развертывания как для поставщиков услуг, так и для предприятий на период совместного использования IPv4 и IPv6.

Для развертывания IPv6 доступны разнообразные механизмы. Эти механизмы включают вручную созданные туннели, такие как сконфигурированные туннели IPv6 и IPv6 поверх IPv4 GRE туннелей, а также полуавтоматические механизмы туннелирования, такие как услуги туннельного брокера, и полностью автоматические механизмы туннелирования, такие как ISATAP и туннели 6в4 (6to4).

Все туннельные механизмы требуют работы конечных точек туннеля в двухстековом режиме. Двухстековые маршрутизаторы, работающие одновременно с обоими протоколами, IPv4 и IPv6, могут непосредственно взаимодействовать как с IPv4, так и с IPv6 конечными системами и маршрутизаторами.

Не все стратегии перехода могут быть применимы ко всем ситуациям и всем сетям. Поскольку ожидается, что, по крайней мере, первоначально, большинство клиентов могут заинтересоваться туннелированием IPv6 поверх их существующих сетей IPv4. Ниже будет представлено сравнение следующих технологий туннелирования IPv6 для использования поверх сетей IPv4:

- вручную сконфигурированный туннель;
- IPv6 поверх IPv4 GRE туннеля;
- автоматический, 1Ру4-совместимый туннель;
- автоматический туннель 6в4 (6to4);
- ISATAP туннель;
- туннель Тередо (Teredo tunnel).

В табл. 6.3 приведены особенности всех перечисленных выше механизмов туннелирования. Каждый механизм имеет свои «за» и «против». Однако, на основании изучения этой таблицы можно сделать важный вывод, который заключается в том, что даже без ручной конфигурации мы можем обеспечить работу оконечных станций и кампусов IPv6 поверх облака IPv4, используя вышеперечисленные механизмы. Для обеспечения безопасности конфигурации туннелей IPv6 поверх IPv4 менеджеры сети могут на конечных маршрутизаторах сконфигурировать IPsec либо для IPv4, либо для IPv6.

Механизмы трансляции IPv6/IPv4. Все эти стратегии интеграции обеспечивают IPv6 из конца в конец. Однако некоторые организации или частные лица могут не захотеть применять любую из этих стратегий трансляции IPv6, поскольку на своих узлах или сетях применяют только IPv6, и не могут применять двойной стек протоколов. Даже если на некоторых узлах или сетях и будет установлен двойной стек протоколов, они могут не иметь IPv4 адресов для использования с двухстековыми узлами. Исходя из этих обстоятельств, взаимодействие между узлами, одни из которых работают только по IPv4, а другие - только по IPv6, требует некоторого уровня трансляции между протоколами IPv6 и IPv4 на хостах или маршрутизаторах или на двухстековых хостах, с прикладным уровнем, понимающим, какой из протоколов использовать. Например, сеть, работающая только по IPv6, все еще может хотеть иметь доступ к ресурсам сети, работающей только по IPv4, к таким как Web-серВера.

Таблица 6.3. **Сравнение различных механизмов туннелирования**

Механизм	Первичное использование	Полезный эффект	Ограничения	Требования
Вручную сконфигурированные туннели IPv6	Устойчивые и безопасные каналы регулярной связи. Соединение с Internet IPv6	Хорошо известная стандартная технология туннелирования. Конечные точки могут быть защищены использованием IPv4 IPsec	Туннель только между двумя точками. Большие издержки на управление	Зарегистрированный IPv6 адрес ISP. Двухстековые маршрутизаторы
IPv6 поверх IPv4 GRE туннеля	Устойчивые и безопасные каналы регулярной связи	Хорошо известная стандартная технология туннелирования. Конечные точки могут быть защищены использованием IPv4 IPsec	Туннель только между двумя точками. Издержки на управление. Реализация GRE туннеля редко доступна на хостах	Зарегистрированный IPv6 адрес ISP. Двухстековые маршрутизаторы. Требуется IS-IS для сконфигурированного по туннелю IPv6
Туннельный брокер	Автономные изолированные IPv6 оконечные системы	Устанавливаемый и управляемый ISP туннель	Косвенное обеспечение потенциальной безопасности	Услуга туннельного брокера должна знать, как создать и отправить скрипт для программного обеспечения
Автоматический IPv4-совместимый туннель	Отдельные хосты или небольшие области. Редкая связь	Автоматический туннель	Связь только с другими IPv4-совместимыми областями. Плохо масштабируем, поскольку предлагает тоже самое адресное пространство, что и IPv4, почти выступая против предпочтительного решения 6в4	Префикс IPv6 (0::/96). Двухстековые маршрутизаторы. Требуется IPv4 адрес для каждого хоста
Автоматический туннель 6в4	Соединение многочисленных удаленных IPv6 доменов. Частая связь	Простота развертывания без издержек на управление	При связи с IPv6 Internet не оптимизирован выбор пути возврата. Потенциальная проблема безопасности, если нет защиты по IPsec (для IPv4 или IPv6)	Префикс IPv6 (2002::/16). Двухстековые маршрутизаторы
ISATAP туннель	Области кампусов. Переход немаршрутизируемых областей	Простое развертывание IPv6 для немногочисленного числа хостов кампуса	Предложенные характеристики канала могут быть не самыми лучшими по сравнению с исходным коммутатором 3-го уровня. Не предлагает решения для широковещательного трафика IPv6	Реализация ISATAP на хостах и маршрутизаторах IPv6. Двухстековые маршрутизаторы
Туннели 6поверх4 (6over4)	Области кампусов. Переход немаршрутизируемых областей	Простое развертывание IPv6 для немногочисленного числа хостов кампуса	Неприемлем, заменен на ISATAP. Требование широковещательности IPv4	—

Различные механизмы трансляции IPv6/IPv4, находящиеся на рассмотрении рабочей группы v6Ops IETF, следующие:

- NAT-Protocol Translation (NAT-PT);
- TCP-UDP relay;
- Bump-in-the-stack (BIS);
- SOCKS-based gateway.

Данные механизмы трансляции протоколов становятся более значимыми, поскольку IPv6 становится все более распространенным и поскольку IPv6 становится протоколом выбора, позволяя традиционным IPv4 системам стать частью общей, всеобъемлющей IPv6 сети.

Механизмы трансляции можно разделить на две категории: те, которые не требуют никаких изменений в хостах IPv4 или IPv6, и те, которые требуют. Примером прежнего подхода является механизм ретрансляции TCP-UDP (TCP-UDP relay), который работает на выделенном сервере и создает отдельные соединения на транспортном уровне с IPv4 и IPv6 хостами, а затем просто передает информацию между ними. Примером более позднего подхода может служить механизм BIS, требующий добавления дополнительных протокольных уровней в протокольный стек IPv4. В механизме BIS между уровнем приложений и сетевым уровнем протокольного стека IPv4 добавляются три дополнительных уровня (названные разрешения расширения, отображения адреса и трансляции). Всякий раз, когда приложению необходимо связаться с хостом, работающим только по IPv6, дополнительные уровни отображают IPv6 адрес в IPv4 адрес хоста IPv4.

В дополнение к стратегиям развертывания IPv6 в среде IPv4, необходим также механизм трансляции протоколов, такой как NAT-PT, для обеспечения связи между приложениями, одни из которых используют только IPv6, а другие - только IPv4 (например, чтобы браузер, работающий только по IPv6, мог связаться с Web-сервером, работающим только по IPv4, или двухстековым сервером). Но здесь есть один недостаток, хорошо известный пользователям NAT – это необходимость в выделенных шлюзах уровня приложения (Application Layered Gateways, ALGs), когда полезная нагрузка приложения включает IP-адрес. Суть механизма, основанного на SOCKS шлюза IPv4/IPv6 состоит в ретрансляции двух законченных IPv4 и IPv6 соединений на прикладном уровне. Данный механизм заключается в дополнительной функциональности обеих конечных систем (клиентов) и двухстекового маршрутизатора (шлюза), позволяющей связываться узлам IPv4 и IPv6. Механизм основан на протоколе SOCKSv5 и наследует все его особенности.

Механизмы трансляции могут быть полезны, так как развертывание IPv6 переходит от тестирования на стадию фактического использования и поскольку (что еще более важно) разработчики приложений решили, что продолжение поддержки IPv4 экономически не

эффективно. В конечном счете, поскольку IPv6 становится протоколом выбора, эти механизмы позволят традиционным системам IPv4 стать частью всеохватывающей сети IPv6. Механизмы трансляции IPv4 и IPv6 на оконечных системах, выделенных серверах, маршрутизаторах сетей IPv6 и вместе на двухстековых хостах обеспечивают полный набор инструментов для возрастающего развертывания IPv6 без разрушения трафика IPv4. Сравнение механизмов трансляции приведено в табл. 6.4.

Развертывание IPv6 по выделенным каналам данных. Многие глобальные сети (WAN) и сети масштаба метрополиса (MAN) были построены с использованием технологий второго уровня, таких как frame relay, ATM, оптических технологий, а кое-где уже начинает использоваться DWDM. На рис. 6.5 представлена типовая конфигурация для IPv6 по выделенным каналам данных.

Маршрутизаторы, подключенные к глобальной сети или метросети поставщика услуг Интернет (ISP), могут быть сконфигурированы для использования той же самой инфраструктуры второго уровня, что и для IPv4, но для работы IPv6, например, поверх выделенной ATM или виртуальных частных каналов (PVC) frame relay, или на различных длинах волны. Такая конфигурация дает дополнительный доход поставщику услуг, не подвергая опасности доходы и трафик IPv4 в связи с интеграцией с IPv6 даже при использовании инфраструктуры второго уровня.

Таблица 6.4. **Сравнение механизмов трансляции протоколов**

Механизм	Первичное использование	Полезный эффект	Ограничения	Требования
NAT-PT	Связь хостов, использующих только IPv6, с хостами, использующими только IPv4	Нет двойного стека	Не обеспечивается IPSec из конца в конец. Выделенный сервер – единственная точка отказа. Технология NAT-PT требует ALG для приложений, включающих IP-адрес	Выделенный сервер. DNS с поддержкой IPv6
TCP-UDP relay	Трансляция между сессиями TCP/UDPv6 и TCP/UDPv4	Свободно распространяемое программное обеспечение	Не обеспечивается IPSec из конца в конец. Выделенный сервер – единственная точка отказа	Выделенный сервер. DNS с поддержкой IPv6
BIS	Связь хостов, использующих только IPv6, с хостами, использующими только IPv4	Реализация в оконечных системах	Все стеки должны быть обновлены	Обновленный стек IPv4
SOCKS-based IPv6/IPv4 gateway	Связь хостов, использующих только IPv6, с хостами, использующими только IPv4	Свободно распространяемое программное обеспечение	Требует дополнительного программного обеспечения для шлюза	Программное обеспечение клиента и шлюза на хосте и маршрутизаторе

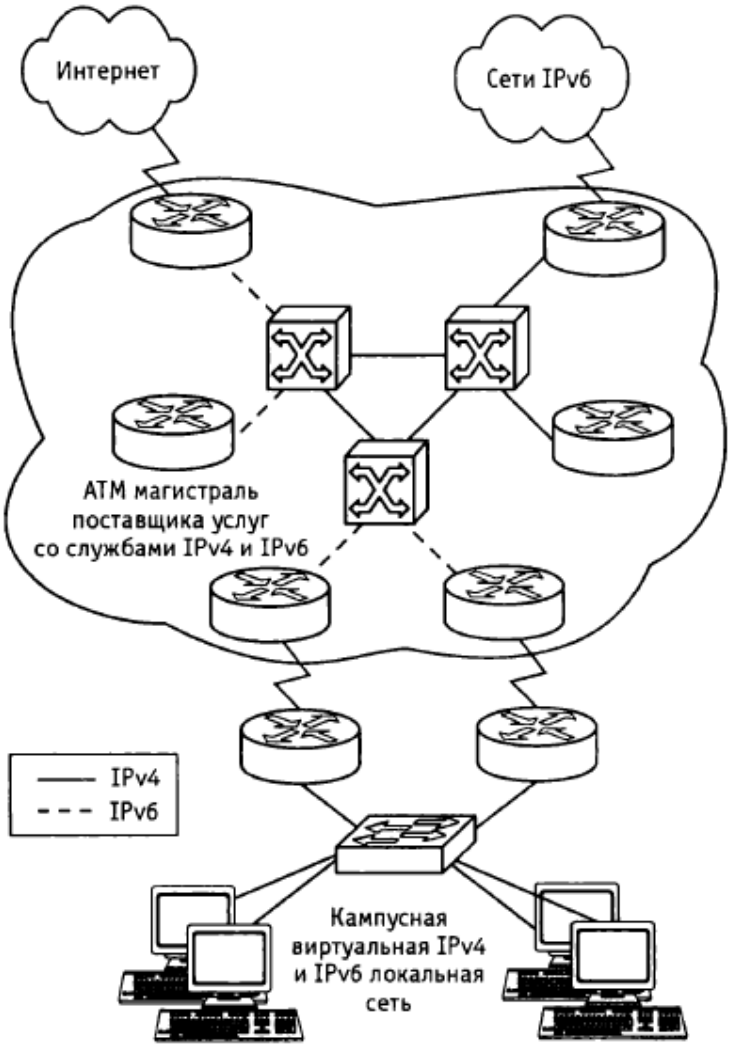


Рис. 6.5. Развертывание IPv6 по выделенным каналам данных

5.2.2. Развертывание IPv6 по магистрали MPLS

IPv6 поверх магистрали MPLS позволяет доменам IPv6 связываться друг с другом через ядро сети IPv4 MPLS. Такое внедрение требует небольшой модернизации инфраструктуры магистрали и не требует реконфигурации маршрутизаторов ядра, так как пересылка основана больше на метках, чем непосредственно на заголовках IP, обеспечивая высокорентабельную стратегию развертывания IPv6. В дополнение к этому, услуги, свойственные виртуальным частным сетям (Virtual Private Network, VPN) и инжинирингу трафика (Traffic Engineering, TE), доступные в среде MPLS, позволяют IPv6 сетям быть объединенными в виртуальные частные сети или экстрасети на инфраструктуре, поддерживающей IPv4 VPNs и MPLS-TE.

Ниже перечислены доступные или находящиеся в разработке стратегии развертывания:

- IPve-туннели на маршрутизаторах на стороне клиента (IPv6 tunnels on customer edge (CE) routers);

- транспорт канала второго уровня через MPLS (Layer 2 circuit transport over MPLS);

- IPv6 на маршрутизаторах на стороне провайдера (IPv6 on provider edge (PE) routers - 6PE);

- добавление IPv6 MPLS VPNs к 6PE (Adding IPv6 MPLS VPNs to 6PE - 6VPE);

- исходная, основанная на MPLS магистраль IPv6 (плоскость управления MPLS основана на IPv6).

Как показано на рис. 6.6, первая из этих стратегий не оказывает влияния и не требует изменений в ядре MPLS, состоящем из маршрутизаторов поставщика (P) и маршрутизаторов на стороне поставщика (PE). Это обеспечивается тем, что эта стратегия использует туннели IPv4 на двухстековых маршрутизаторах на стороне клиента (CE) для инкапсуляции трафика IPv6, который, таким образом, внутри сети MPLS появляется как трафик IPv4. Вторая стратегия не требует никаких изменений в базовых механизмах маршрутизации. Третья и четвертая стратегии требуют изменений в маршрутизаторах на стороне поставщика (PE) для поддержки двойного стека, но все функции ядра, т. е. маршрутизаторов поставщика (P) остаются на уровне IPv4. Последняя из стратегий предполагает работу собственного IPv6 MPLS ядра, но данная стратегия требует полной сетевой модернизации всех маршрутизаторов (как P, так и PE) с двойными плоскостями управления для IPv4 и для IPv6. В табл. 6.5 представлено сравнение этих стратегий для транспортировки IPv6 по магистрали MPLS. Ниже каждый из этих механизмов будет рассмотрен более подробно.

IPv6 по транспортному каналу второго уровня по MPLS. Использование любого канального транспорта для развертывания IPv6 по сетям MPLS не оказывает влияния на работу и инфраструктуру MPLS. Такой метод не требует изменений ни в маршрутизаторах P ядра, ни в маршрутизаторах PE (для поддержки одного из механизмов канального транспорта второго уровня поверх MPLS), соединенных с пользователями. Связь между удаленными доменами IPv6 обеспечивают исходные протоколы IPv6 по выделенным каналам, где основные механизмы полностью прозрачны для IPv6. Трафик IPv6 туннелируется с использованием любого транспорта поверх MPLS (Any Transport Over MPLS - AToM) или Ethernet по MPLS (Ethernet over MPLS - EoMPLS) с помощью IPv6 маршрутизаторов, подключенных через ATM или Ethernet интерфейсы соответственно.

На рис. 6.7 приведен пример развертывания IPv6 по любому каналу транспорта по MPLS.

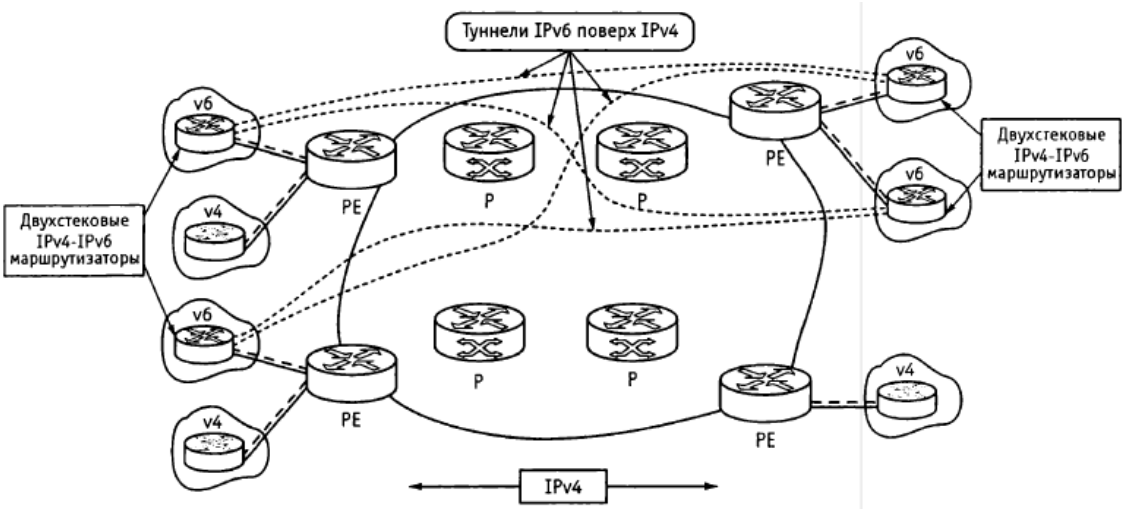


Рис. 6.6. Развертывание IPv6 с использованием туннелей на CE маршрутизаторах

Таблица 6.5. **Сравнение различных механизмов передачи IPv6 по магистрали MPLS**

Механизм	Первичное использование	Полезный эффект	Ограничения	Требования
Использование IPv6 туннелей на маршрутизаторах CE	Корпоративные клиенты, желающие использовать IPv6 поверх существующих услуг MPLS	Не оказывает влияния на инфраструктуру MPLS	Проблема масштабируемости при росте числа туннелей между CE	Двухстековые маршрутизаторы CE
Транспорт канала второго уровня через MPLS	Поставщик услуг с ATM или Ethernet каналами к маршрутизаторам CE	Полностью прозрачная IPv6 связь	Нет смешения IPv4 и IPv6 трафика	Необходим транспорт второго уровня по MPLS
IPv6 на маршрутизаторах на стороне провайдера (6PE) поверх MPLS	Поставщики услуг Интернет и поставщики мобильных услуг, желающие предлагать услуги IPv6	Дешевая и низкорисковая модернизация маршрутизаторов PE без воздействий на ядро MPLS	Применимо только к инфраструктуре MPLS	Модернизация программного обеспечения маршрутизаторов PE
IPv6 VPN на маршрутизаторах на стороне провайдера (6VPE) поверх MPLS	Поставщики услуг Интернет и поставщики мобильных услуг, желающие предлагать услуги IPv6 VPN	Дешевая и низкорисковая модернизация маршрутизаторов PE без воздействий на ядро MPLS	Применимо к инфраструктуре MPLS, хотя может быть исполнено и для других механизмов туннелирования. Утечка IPv6 адреса из глобальной маршрутной таблицы должна хорошо контролироваться	Поддержка VPN или VRF

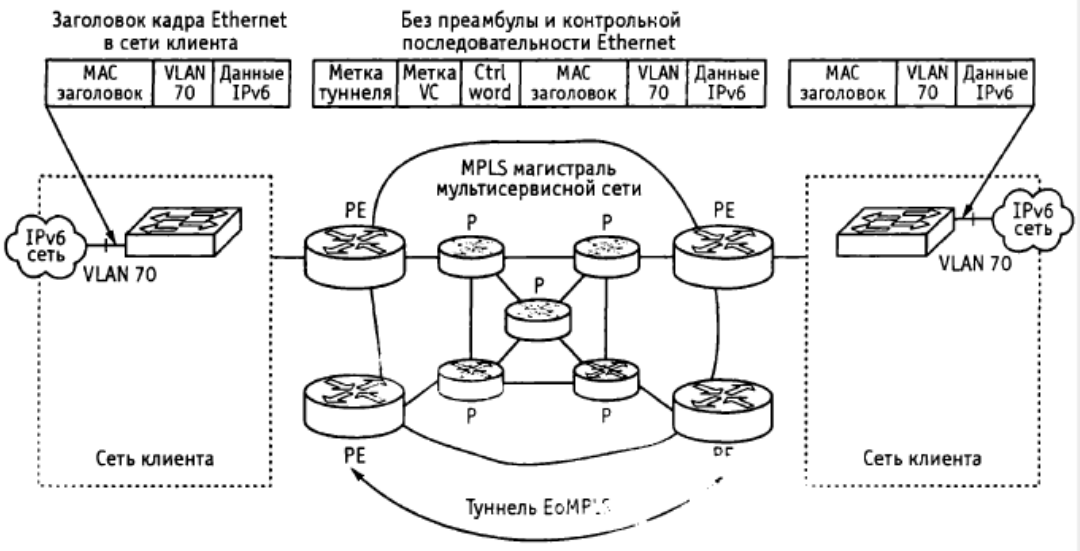


Рис. 6.7. IPv6 по «Ethernet по MPLS»

IPv6 на маршрутизаторах на стороне провайдера (PE). Другая стратегия развертывания заключается в конфигурировании IPv6 на MPLS PE маршрутизаторах. Данная стратегия имеет основное преимущество для поставщиков услуг, при которой нет необходимости в модернизации ни аппаратных, ни программных средств P маршрутизаторов в ядре MPLS сети, что, таким образом устраняет влияние на доход, генерируемый существующим IPv4 трафиком. Стратегия сохраняет выгоды от текущих особенностей IPv4 MPLS (например, MPLS-TE или VPN) наряду с появлением возможности предоставления исходных IPv6 услуг для корпоративных клиентов (используя поставляемые ISP IPv6 префиксы). Архитектура 6PE разрешает поддержку VPN для IPv6. На рис. 6.8 приведен пример развертывания IPv6 на маршрутизаторах PE.

Пересылка IPv6 данных выполняется благодаря коммутации по меткам, устраняя потребность как в туннелях IPv6 поверх IPv4, так и в дополнительной инкапсуляции 2-го уровня, разрешая появление исходных услуг IPv6, которые можно предлагать по всей сети и масштабировать, поскольку число пользователей IPv6 растет, в то время как технологии, такие как отражатели маршрутов, могут быть сконфигурированы позже.

Каждый маршрутизатор PE, который должен поддерживать IPv6 соединения, нуждается в модернизации до двухстекового (становится 6PE маршрутизатором) и конфигурируется для работы с MPLS на интерфейсах, соединяющих его с маршрутизаторами ядра P. В зависимости от требований области применения, каждый маршрутизатор может быть сконфигурирован для пересылки IPv6 или IPv6 и IPv4 трафика на интерфейсах к маршрутизаторам CE, таким образом, обеспечивая возможность предоставления либо только исходных услуг IPv6, либо одновременно услуг IPv4 и IPv6. Маршрутизатор 6PE обменивается как IPv4, так и IPv6 маршрутной информацией по любому из поддерживаемых протоколов маршрутизации, в зависимости от соединения, и переключает IPv4 и IPv6 трафик по исходным IPv4 и IPv6 интерфейсам, не работающим по MPLS.

Маршрутизатор 6PE обменивается информацией о доступности с другими 6PE маршрутизаторами в домене MPLS, используя мультипротокольный граничный шлюзовой протокол (Border Gateway Protocol, BGP) и совместно использует с другими P или PE устройствами домена общий протокол маршрутизации IPv4, такой как открытый протокол «кратчайший путь выбирается первым» (Open Shortest Path First, OSPF) или интегрированный протокол «промежуточная система - промежуточная система» (Intermediate System to Intermediate System, IS-IS). Маршрутизаторы 6PE инкапсулируют трафик IPv6, используя два уровня меток MPLS. Высшая метка распределяется в соответствии с протоколом распределения меток (Label Distribunion Protocol, LDP) или протокола распределения тегов (Tag Distribution Protocol, TDP), используемых устройствами ядра для

переноса пакетов к назначенному 6PE в соответствии с маршрутной информацией IPv4. Вторая или низшая метка связана с префиксом адреса IPv6 пункта назначения через мультипротокол BGP-4, обеспечивая выполнение баланса нагрузки.

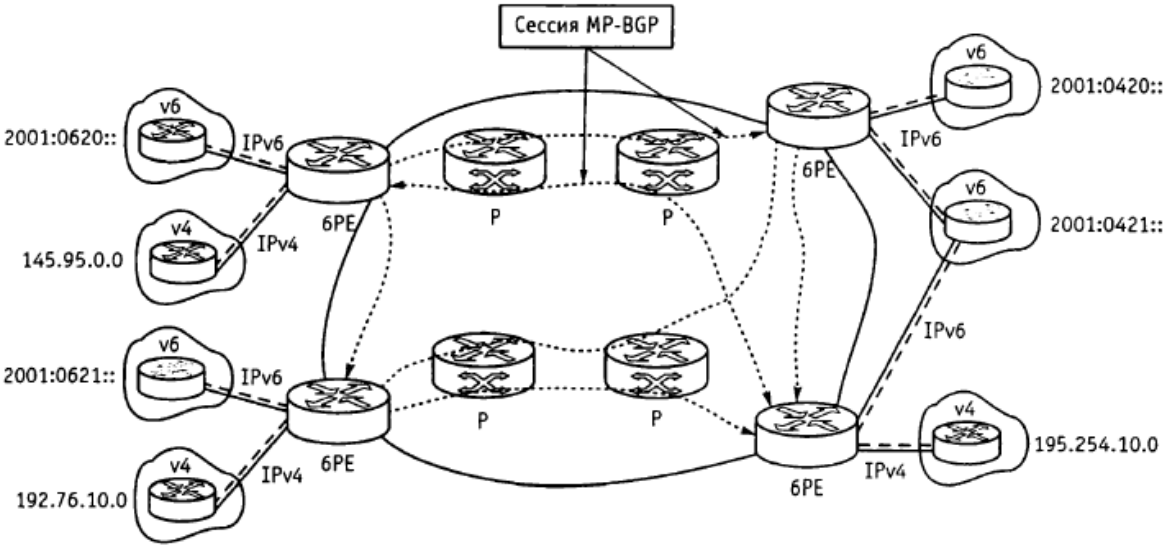


Рис. 6.8. IPv6 на маршрутизаторах на стороне провайдера (PE)

Маршрутизаторы IPv6 VPN на стороне провайдера по магистрали MPLS. Поставщики услуг, предлагающие своим клиентам услуги MPLS/VPN, могут ожидать добавления услуг IPv6/VPN к их портфелю услуг. Как ожидается, VPN станут IPv6/VPN, когда CE маршрутизаторы будут поддерживать исходный IPv6 на интерфейсах или подынтерфейсах к маршрутизаторам PE. Добавление IPv6/VPN способностей 6PE маршрутизатору, называемому в таком случае 6VPE для IPv6 VPN маршрутизатором на стороне поставщика поверх MPLS, является альтернативой, позволяющей для ISP предоставлять подобные услуги и по IPv4. Подобно IPv4/VPN распределению маршрутов, BGP и его расширения используются для распределения маршрутов от областей IPv6/VPN ко всем другим 6VPE маршрутизаторам, соединенным с той же самой областью IPv6/VPN. PE используют таблицы VPN маршрутизации и форвардинга (VPN Routing and Forwarding - VRF) для раздельного обслуживания информации о доступности и информацию о пересылке данных для каждой IPv6 VPN, как показано на рис. 6.9.

Когда 6VPE1 получает IPV6 пакет от CE A, он ищет адрес пункта назначения пакета IPv6 в таблице VRF A. Это позволяет ему найти VPNIPv6 маршрут, который будет иметь соответствующую MPLS метку и соответствующее значение BGP next hop. Метка MPLS накладывается на IPv6 пакет. 6VPE1 непосредственно выдвигает другую метку, верхняя метка присваивается с помощью LDP/IGPv4 адресу IPv4 следующего «прыжка» BGP (BGP next hop) для достижения 6VPE2 через MPLS облако на стеке меток промаркированного пакета IPv6/VPN. Эта самая верхняя налагаемая метка соответствует траектории

маркированного маршрута (Label Switched Path, LSP), начинающегося на 6VPE1 и заканчивающегося на 6VPE2. Как было упомянуто выше, нижняя метка связана с префиксом IPv6 VPN через BGP.

Все P маршрутизаторы в ядре сети коммутируют VPN пакеты, основываясь только на верхней метке стека, которая указывает на встречный маршрутизатор 6VPE2. Так как в соответствии с нормальными правилами перенаправления MPLS, P маршрутизаторы никогда не смотрят дальше первой метки, то, таким образом, полностью ничего не знают о второй метке или о переносимом через магистраль сети IPv6 VPN пакете.

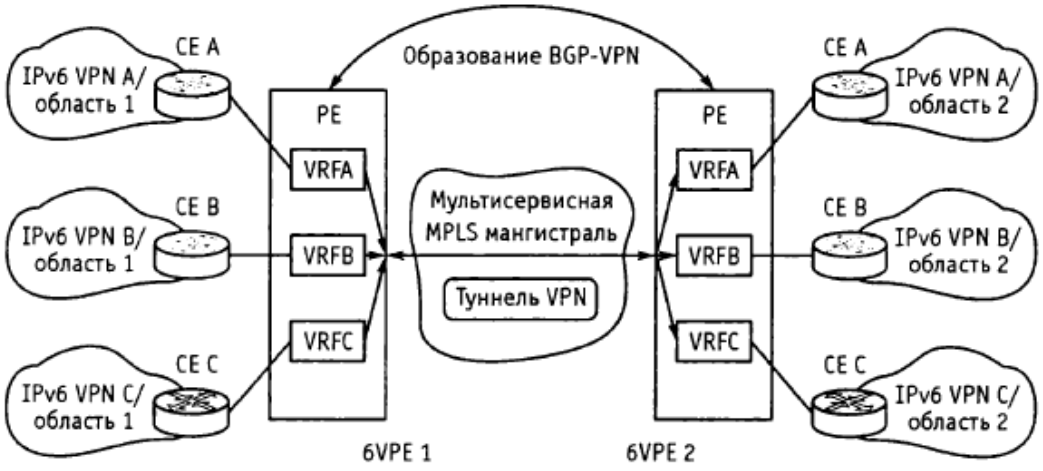


Рис. 6.9. Архитектура IPv6 MPLS VPN

Таблица 6.6 **Сравнение всех стратегий развертывания или механизмов перехода**

Стратегия развертывания	Ключевые пользователи и первичное использование	Полезный эффект	Ограничения	Требования
IPv6 по туннелям IPv4	Поставщики услуг, желающие предоставлять исходные услуги IPv6. Организации, желающие связать домены или каналы IPv6 с удаленными IPv6 сетями	Может продемонстрировать требования минимальных инвестиций. Простота осуществления поверх существующей инфраструктуры IPv4. Низкая стоимость и низкий риск	Комплексное управление и диагностика благодаря независимости туннельной и канальной топологий	Доступ к IPv4 через двухстековые маршрутизаторы с IPv4 и IPv6 адресами. Доступ к IPv6 DNS
IPv6 по выделенным каналам данных	Поставщики услуг глобальных или метросетей, развертывающие ATM, Frame Relay или DWDM	Может предоставлять IPv6 из конца в конец без воздействия на трафик и доходы IPv4	—	Доступ к WAN через двухстековые маршрутизаторы, с IPv4 и IPv6 адресами. Доступ к IPv6 DNS
IPv6 по магистралям MPLS	Поставщики мобильных услуг или существующие региональные поставщики услуг, развертывающие MPLS	Интегрирует IPv6 по MPLS так, что не требуется модернизации аппаратного или программного обеспечения ядра	Реализация требует работы MPLS. Высокие затраты на управление	Минимальные изменения маршрутизаторов клиентов (CE) и граничных маршрутизаторов поставщика (PE), зависящие от технологии
Двухстековые магистрали	Небольшие сети организаций. Инфраструктура поставщиков услуг. Инфраструктура корпоративной WAN. Инфраструктура кампуса	Простота применения для малых кампусных сетей со смешением IPv4 и IPv6 приложений. Возможность предоставлять одинаковые услуги (multicast, QoS) и для IPv4 и для IPv6	Комплексное управление протоколами маршрутизации. Огромный объем модернизации для больших сетей	Сетевые устройства должны быть совместимы с двойным стеком. Доступ к IPv6 DNS. Проект сети должен быть применим к обеим версиям IP с достаточной памятью таблиц маршрутизации

Выходной PE маршрутизатор, 6VPE2, получая маркированный IPv6 VPN пакет, отбрасывает первую метку и выполняет поиск по второй метке, которая уникально идентифицирует нужную VRF A, а иногда даже и исходящий интерфейс на 6VPE2. По

выполнении поиска в необходимой VRF A, IPv6 пакет посылается к надлежащему CE маршрутизатору в домене или области IPv6.

5.2.3. Рассмотрение проектов IPv6 сетей

Развертывание IPv6, когда проектировщики сети одобряют стратегию интеграции IPv6, которая начинается с границ сети и движется к центру, позволяет контролировать затраты на развертывание и сосредоточиться на потребностях приложений, а не на выполнении полной модернизации до исходной IPv6 сети на данной стадии. Различные стратегии развертывания разрешают сейчас первые шаги перехода к IPv6 либо как испытание возможностей IPv6, или как ранние контролируемые стадии использования IPv6 как основной сети. В табл. 6.6 приведено сравнение различных стратегий развертывания.

5.2.4. Развертывание IPv6 в сетевой среде поставщика услуг

Поставщик услуг как администратор сети может захотеть оценить применение IPv6 сейчас, потому что текущее распределенное адресное пространство может быть не в состоянии удовлетворить потенциально огромное увеличение числа пользователей или запросы новых технологий от конечных клиентов, которые могут открыть новые возможности бизнеса для поставщика услуг. Использование уникальных глобальных IPv6 адресов предоставляет благоприятные возможности для создания новых бизнес-моделей, добавляет доходы и увеличивает портфель услуг. Определенный для будущего Интернет, для наших следующих поколений, IPv6 может использоваться для достижимости и обеспечения безопасности из конца в конец для вновь появляющихся сетевых устройств, таких как карманные персональные компьютеры с возможностью подключения к Интернет, домашние компьютерные сети (HAN), подключенные к Интернет автомобили, интегрированные телефонные услуги и распределенные игры.

Нужно рассматривать развертывание IPv6 относительно трех нижеперечисленных стадий, сосредотачиваясь на бизнес модели, которая поможет управляющему звену увидеть дополнительное значение проекта. В данном контексте настоятельно рекомендуется, чтобы IPv6 была двухстековой IPv4/IPv6 услугой, когда операторы имеют достаточно опыта работы с двойным стеком.

Предоставление IPv6 сервиса (включая двухстековый сервис IPv4 и IPv6) на уровне доступа клиента. Начало развертывания IPv6 на уровне доступа клиента позволяет предоставлять IPv6 услуги уже сейчас без основной модернизации инфраструктуры ядра и без воздействия на текущие IPv4/MPLS услуги. Данный подход позволяет произвести оценку продуктов и услуг IPv6 до их окончательного развертывания на сети и оценить будущие требования для IPv6 без солидных инвестиций на этой ранней стадии.

Работа IPv6 (включая двухстековый сервис IPv4 и IPv6) непосредственно в инфраструктуре ядра. По завершении данной стадии, поскольку системы управления сетью полностью охвачены IPv6, сетевая инфраструктура может быть модернизирована для поддержки IPv6.

Взаимодействие с другими поставщиками услуг IPv6. Взаимодействие с другими поставщиками услуг IPv6 или 1Ру6-магистралью (бBone) позволяет дальнейшее оценивание и дает лучшее понимание требований к IPv6.

Сегодня Интернет не воспринимается как достаточно надежная сеть для передачи трафика реального времени. Но это происходит не из-за недостатка перспективных механизмов, таких как потоковые слежение и ограничение (shaping/policing), а из-за сложности выбора метода обеспечения QoS сети и компромисса между простотой и большей управляемостью. Хороший проект сети, простота, высокая доступность и обеспечение защиты являются ключевыми аспектами обеспечения QoS на магистралях Интернет. Хороший проект сети плюс некоторая степень резервирования ресурсов не только делают сеть более отказоустойчивой, но также и предотвращают многие проблемы, связанные с QoS, и устраняют потребность в сложных механизмах, разработанных для их решения. Это делает сеть более простой и увеличивает ее доступность. Три класса трафика (Premium, Assured, и Best effort) достаточны для удовлетворения обозримых потребностей клиентов. Различные классы трафика будут обслуживаться по-разному, особенно при неблагоприятных сетевых условиях. Быстрая перемаршрутизация MPLS или другие механизмы защиты могут использоваться для защиты Premium-трафика при отказах маршрутизаторов или каналов. При возникновении неисправностей в одной части сети инжиниринг трафика должен использоваться для перемещения трафика в другую часть сети. DiffServ инжиниринг трафика может использоваться для предотвращения концентрации высокоприоритетного трафика на любом канале, так что высокопроизводительный трафик будет иметь низкую задержку и джиттер, и при необходимости может обрабатываться предпочтительно за счет трафика других классов. Схемы управления трафиком на магистрали, такие как Policing и Shaping, должны применяться для микроконтроля и использоваться, когда инжиниринг трафика становится недостаточным.

6. Компьютерные лабораторные работы и компьютерный практикум

6.1. Проектирование защищенной IP-АТС на базе программного обеспечения ASTERISK

Целью данной курсовой работы является проектирование АТС на основе протокола IP, на базе операционной системы Windows и программного обеспечения Asterisk. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям. Организация сети телефонной связи сводится к таким вопросам как обеспечение качества услуг, предоставляемых абонентам, а так же защищенности конфиденциальной информации, которая может передаваться по речевым каналам. Для того чтобы начать проектирование такой системы, необходимо разработать ее структуру, зафиксировать основные функции, определить актуальные угрозы.

Аналитический обзор

VoIP: наведение мостов между традиционной и сетевой телефонией.

Хотя передача голоса по IP-протоколу (Voice over IP, VoIP) часто рассматривается как своего рода бесплатная междугородняя телефонная связь, настоящая ценность VoIP в том, что с его помощью голос становится всего лишь обычным приложением в сети передачи данных. Кажется, мы забыли о том, что назначение телефона – позволить людям общаться. Это простая цель на самом деле, и мы должны иметь возможность реализовывать ее намного более гибко и творчески, чем это предлагается сейчас. Поскольку отрасль продемонстрировала нежелание стремиться к данной цели, решением задачи занялись энтузиасты. Сложность состоит в том, что отрасль, которая практически не изменилась за последние сто лет, не проявляет особого интереса к этому и сейчас.

Проект телефонной связи Zapata (Zapata Telephony Project) был основан Джимом Диксоном, инженером-консультантом по связи. Его вдохновило невероятное увеличение частот ЦП (центрального процессора), которое в компьютерной отрасли сейчас уже воспринимается как должное. Диксон считал, что при наличии плат, включающих только базовые электронные компоненты, необходимые для взаимодействия с телефонной сетью, можно было бы создать намного более экономичные системы телефонной связи. Дорогие компоненты не нужны, потому что вся цифровая обработка сигнала (Digital Signal Processing, DSP – ЦОС) происходила бы в ЦП под управлением программного обеспечения. При этом нагрузка на ЦП сильно возросла бы, но Диксон был уверен, что низкая стоимость ЦП по сравнению с их производительностью делает их применение намного более привлекательным, чем использование ЦОС, и, что еще более важно, соотношение цена/производительность продолжало бы улучшаться с повышением мощности ЦП. Как все мечтатели, Диксон верил, что эта идея откроется многим и ему просто надо подождать, пока

кто-нибудь другой не реализует то, что он видел как очевидное усовершенствование. Но через несколько лет такие платы не только не были созданы, но, казалось, никто и не собирался ими заниматься. Тогда ему стало ясно, что если он хочет совершить революцию, то должен начинать ее самостоятельно. И родился проект телефонной связи Zapata.

Общие принципы IP-телефонии

Принципы пакетной передачи речи

«Классические» телефонные сети основаны на технологии коммутации каналов (рисунок 6.1), которая для каждого телефонного разговора требует выделенного физического соединения. Следовательно, один телефонный разговор представляет собой одно физическое соединение телефонных каналов. Основным недостатком телефонных сетей с коммутацией каналов является неэффективное использование полосы канала – во время пауз в речи канал не несет никакой полезной нагрузки.

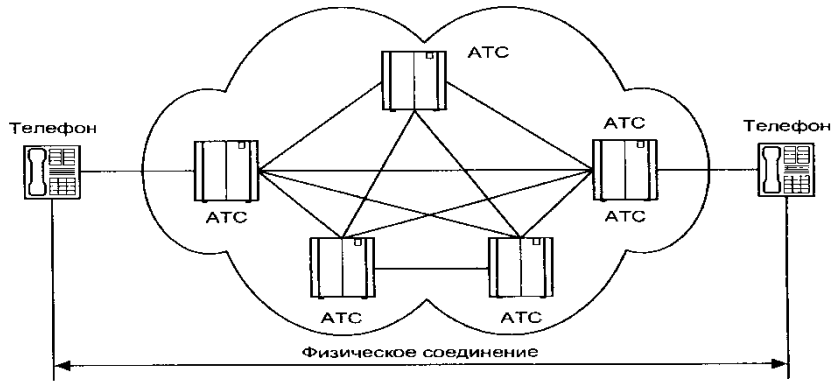


Рис. 6.1. Соединение в «классической» телефонной сети

Переход от аналоговых к цифровым технологиям стал важным шагом для возникновения современных цифровых телекоммуникационных сетей. Одним из таких шагов в развитии цифровой телефонии стал переход к пакетной коммутации. В сетях пакетной коммутации по каналам связи передаются единицы информации, которые не зависят от физического носителя. Такими единицами могут быть пакеты, кадры или ячейки (в зависимости от протокола), но в любом случае они передаются по разделяемой сети (рисунок 3.2), более того - по отдельным виртуальным каналам, не зависящим от физической среды. Каждый пакет идентифицируется заголовком, который может содержать информацию об используемом им канале, его происхождении (то есть об источнике или отправителе) и пункте назначения (о получателе или приемнике).

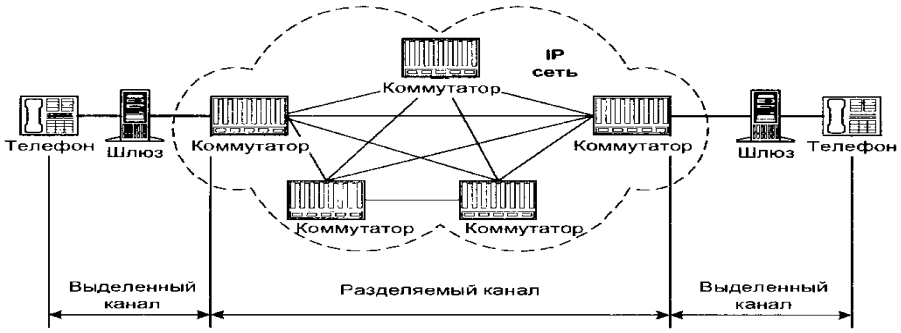


Рис. 6.2. Соединение в сети с коммутацией пакетов

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Любой компьютер и терминал такой сети имеет свой уникальный IP-адрес, и передаваемые пакеты маршрутизируются к получателю в соответствии с этим адресом, указываемом в заголовке. Данные могут передаваться одновременно между многими пользователями и процессами по одной и той же линии. При возникновении проблем IP-сети могут изменять маршрут для обхода неисправных участков. При этом протокол IP не требует выделенного канала для сигнализации.

Процесс передачи голоса по IP-сети состоит из нескольких этапов.

На первом этапе осуществляется оцифровка голоса. Затем оцифрованные данные анализируются и обрабатываются с целью уменьшения физического объема данных, передаваемых получателю. Как правило, на этом этапе происходит подавление ненужных пауз и фонового шума, а также компрессирование.

На следующем этапе полученная последовательность данных разбивается на пакеты и к ней добавляется протокольная информация - адрес получателя, порядковый номер пакета на случай, если они будут доставлены не последовательно, и дополнительные данные для коррекции ошибок. При этом происходит временное накопление необходимого количества данных для образования пакета до его непосредственной отправки в сеть.

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов. Когда голосовые пакеты приходят на терминал получателя, то сначала проверяется их порядковая последовательность. Поскольку IP-сети не гарантируют время доставки, то пакеты со старшими порядковыми номерами могут прийти раньше, более того, интервал времени получения также может колебаться. Для восстановления исходной последовательности и синхронизации происходит временное накопление пакетов. Однако некоторые пакеты могут быть вообще потеряны при доставке, либо задержка их доставки превышает допустимый разброс. В обычных условиях приемный терминал запрашивает повторную передачу ошибочных или потерянных данных. Но передача голоса слишком

критична ко времени доставки, поэтому в этом случае либо включается алгоритм аппроксимации, позволяющий на основе полученных пакетов приблизительно восстановить потерянные, либо эти потери просто игнорируются, а пропуски заполняются данными случайным образом.

Полученная таким образом (не восстановленная) последовательность данных декомпрессируется и преобразуется непосредственно в аудио-сигнал, несущий голосовую информацию получателю.

Таким образом, с большой степенью вероятности, полученная информация не соответствует исходной (искажена) и задержана (обработка на приёмной и передающей сторонах требует промежуточного накопления). Однако в некоторых пределах избыточность голосовой информации позволяет мириться с такими потерями.

Абонент, оплативший полосу 64 кбит/с, использует канал в среднем лишь на 25 %. Значит, оператор способен продать имеющийся у него ресурс в четыре раза большему числу пользователей, не перегружая свою сеть. Это выгодно обеим сторонам – и клиенту, и продавцу, - поскольку оператор увеличивает свои доходы и уменьшает абонентскую плату за счёт снижения издержек.

В настоящее время, в IP-телефонии существует два основных способа передачи голосовых пакетов по IP-сети:

- через глобальную сеть Интернет (Интернет-телефония);

- использую сети передачи данных на базе выделенных каналов (IP-телефония);

В первом случае, полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику, а значит, задержки при прохождении пакетов могут быть самыми разными. При использовании же выделенных каналов исключительно для голосовых пакетов можно гарантировать фиксированную (или почти фиксированную) скорость передачи. Ввиду широкого распространения сети Интернет особый интерес вызывает реализация системы Интернет-телефонии, хотя в этом случае качество телефонной связи оператором не гарантируется.

Для того чтобы осуществить междугородную (международную) связь с помощью телефонных серверов, оператор услуги должны иметь по серверу в тех местах, куда и откуда планируются звонки. Стоимость такой связи на порядок меньше стоимости телефонного звонка по обычным телефонным линиям.

Общий принцип действия телефонных серверов Интернет-телефонии таков: с одной стороны, сервер связан с телефонными линиями и может соединиться с любым телефоном мира. С другой стороны, сервер связан с Интернетом и может связаться с любым компьютером в мире. Сервер принимает стандартный телефонный сигнал, оцифровывает его

(если он исходно не цифровой), значительно сжимает, разбивает на пакеты и отправляет через Интернет по назначению с использованием протокола IP. Для пакетов, приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке. Обе составляющие операции (вход сигнала в телефонную сеть и его выход из телефонной сети) происходят практически одновременно, что позволяет обеспечить полнодуплексный разговор. На основе этих базовых операций можно построить много различных конфигураций. Например, звонок «телефон-компьютер» или «компьютер-телефон» может обеспечивать один телефонный сервер. Для организации связи телефон (факс)-телефон (факс) нужно два сервера.

С точки зрения масштабируемости (если отвлечься от проблем с неконтролируемым ухудшением качества при росте нагрузки на сеть) IP-телефония представляется вполне законченным решением. Во-первых, поскольку соединение на базе протокола IP может начинаться (и заканчиваться) в любой точке сети от абонента до магистрали. Соответственно, IP-телефонию в сети можно вводить участок за участком, что, кстати, на руку и с точки зрения миграции, так как ее можно проводить «сверху вниз», «снизу вверх» или по любой другой схеме. Для решений IP-телефонии характерна определенная модульность: количество и мощность различных узлов - шлюзов, gatekeeper («привратников» - так в терминологии VoIP именуются серверы обработки номерных планов) - можно наращивать практически независимо, в соответствии с текущими потребностями.

Межсетевой протокол IP

В настоящее время наиболее эффективная передача потока любых дискретных (цифровых) сигналов, в том числе и несущих речь (голос), обеспечивается цифровыми сетями электросвязи, в которых реализована пакетная технология IP.

Протокол IP – основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения.

Следует подчеркнуть, что протокол IP реализуется не только в глобальной сети Интернет, для которой он был первоначально разработан, он может быть применен и в других цифровых телекоммуникационных сетях.

Основным сдерживающим фактором на пути масштабного внедрения IP-телефонии является отсутствие в протоколе IP механизмов обеспечения гарантированного качества услуг, что делает его пока не самым надежным транспортом для передачи голосового трафика. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. Сам протокол IP не гарантирует доставку пакетов, а также время их доставки, что вызывает такие проблемы, как «рваный голос» и

просто провалы в разговоре. В протоколе IP нет механизмов, обычно применяемых для увеличения достоверности конечных данных: отсутствует квитирование – обмен подтверждениями между отправителем и получателем, нет процедуры упорядочения, повторных передач или других подобных функций. Если во время продвижения пакета произошла какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки. Например, если на промежуточном маршрутизаторе пакет был отброшен по причине истечения времени жизни или из-за ошибки в контрольной сумме, то модуль IP не пытается заново послать испорченный или потерянный пакет. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP.

IP-адрес

Администратор сети присваивает оконечным устройствам IP-адреса в соответствии с тем, к каким IP-сетям они подключены. Для IP-адреса первоначально выбрали размер в 32 бита для удобства его обработки в 32 – разрядном регистре компьютера. Для обеспечения свойства иерархичности адрес содержит две части: номер сети и номер узла (рисунок 2.3). Число бит, отводимых для этих номеров, может быть переменным.

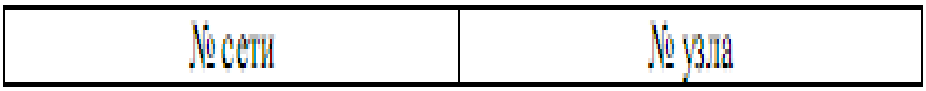


Рис. 6.3. Структура IP-адреса

Для того, чтобы можно было присваивать адреса и малым и большим сетям, ввели несколько классов адресов: A, B, C (рисунок. 2.4).

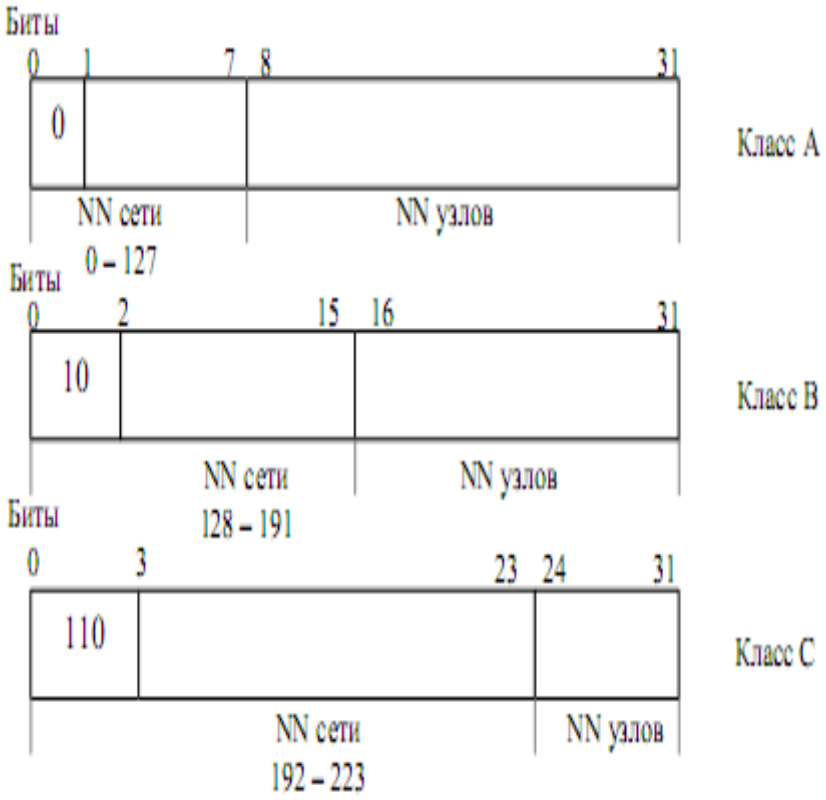


Рис. 6.4. Адреса класса A, B, C

1. Адреса класса A предназначены для организации очень больших сетей. Они обязательно начинаются с 0. Всего таких сетей 128. В каждой из них может быть 16777216 (2^{24}) адресов станций (узлов) и их объем составляет 50 % от общего количества всех IP-адресов.

2. Адреса класса B тоже дают возможность организовать достаточно большие сети в диапазоне номеров 128 – 191. Здесь под номер сети отводится уже два байта. Число сетей здесь – 2^{14} = 16384, а максимальное число узлов в сети – 2^{16} = 65536. Объем адресов класса B составляет 25 %.

3. Адреса класса C содержат три байта для номера сети и один байт для номера узла. Следовательно в одной сети класса C может быть не более 2^{8} = 256 адресов, а таких сетей довольно много – 2^{21} = 2097152. Сети класса C – это небольшие сети.

Кроме классов A, B, C существуют специальные классы D и E. Адреса класса D (224 – 239) используются для многоадресных рассылок в IP-сетях, когда одно сообщение распространяется среди группы разбросанных по сети станций. Адреса класса E(240 – 255) составляют резерв, который может использоваться в экспериментальных целях.

Описание основных протоколов систем IP-телефонии

Стандарт H.323

Набор рекомендаций МСЭ-Т H.323 определяет сетевые компоненты, протоколы и процедуры, позволяющие организовать мультимедиа-связь в пакетных сетях, в том числе в ЛВС Ethernet. Они определяют порядок функционирования абонентских терминалов в сетях с разделяемым ресурсом, не гарантирующих качества обслуживания QoS. H.323-совместимые устройства могут применяться для телефонной связи (IP-телефония), передачи звука и видео (видеотелефония), а также звука, видео и данных (мультимедийные конференции).

В связи с появлением множества аппаратно-программных средств организации телефонной связи по протоколу IP потребовалось внести изменения в спецификации H.323, так как эти средства зачастую оказывались несовместимыми друг с другом. В частности, понадобилось обеспечить взаимодействие телефонных устройств на базе ПК и обычных телефонов для сетей, функционирующих по принципу коммутации каналов. Стандарт H.323 входит в семейство рекомендаций H.32x, описывающих порядок организации мультимедиа-связи в сетях различных типов:

H.320 - узкополосные цифровые коммутируемые сети, включая -ISDN;

H.321 - широкополосные сети ISDN и ATM;

H.322 - пакетные сети с гарантированной полосой пропускания;

H.324 - телефонные сети общего пользования (ТфОП).

Одна из основных целей разработки стандарта H.323 - обеспечение взаимодействия с другими типами сетей мультимедиа-связи (рисунок 3.1). Данная задача реализуется с помощью шлюзов, осуществляющих трансляцию сигнализации и форматов данных. Стандарт H.323 позволяет создать надежные решения для организации коммуникаций по ненадежным сетям с переменной задержкой. При условии соответствия стандарту устройства с различными возможностями могут и взаимодействовать друг с другом. Например, терминалы с видео средствами могут участвовать в аудиоконференции. В совокупности с другими стандартами МСЭ-Т на мультимедийную связь и телеконференции рекомендации H.323 применимы для любых видов соединений - от многоточечных до соединений «точка-точка». Основные компоненты этого стандарта приведены в таблице 6.1.

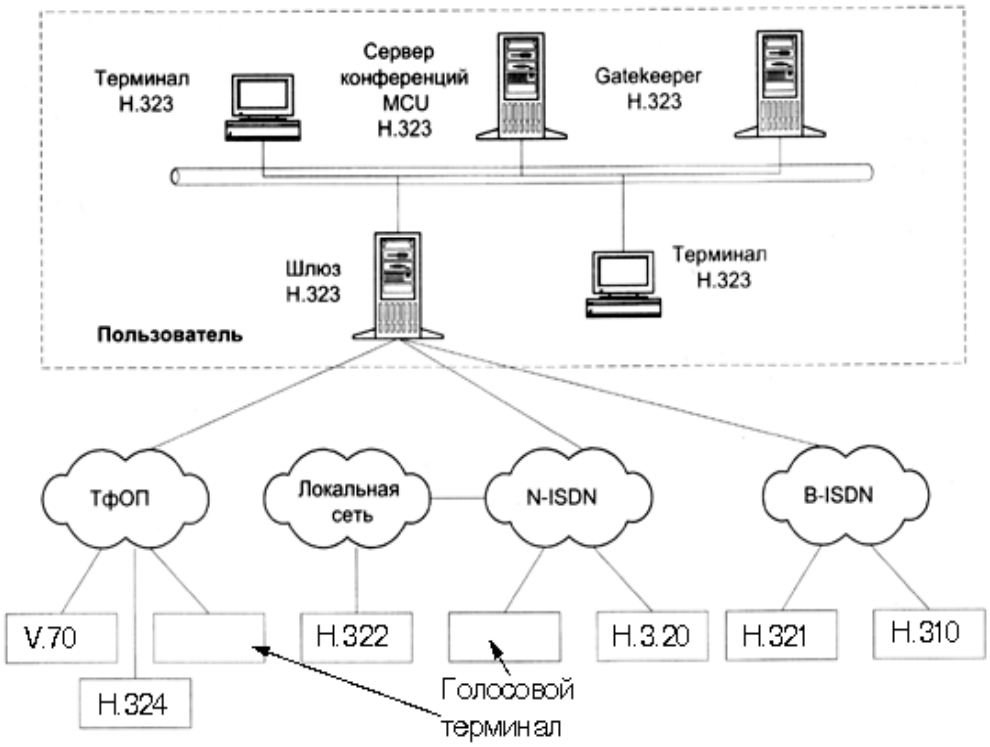


Рис. 6.5. Конфигурация сети на базе стандарта H.323

Стандарт H. 323 определяет также порядок взаимодействия с оконечными устройствами других стандартов. Наиболее часто такая задача возникает при сопряжении телефонных сетей с коммутацией пакетов и коммутацией каналов. Сети стандарта H.323 совместимы и с другими типами H.32x-сетей. Межсетевое взаимодействие различных H.32x-сетей определяет рекомендация H.246. На следующем этапе развития IP-телефонии к спецификациям H.323, соответствующим нижним уровням эталонной модели взаимодействия открытых систем (ЭМВОС), будут добавлены новые. Они зафиксируют возможности обеспечения классов (class-of-service, CoS) и качества обслуживания (quality-of-service, QoS), т. е. услуг, относящихся, соответственно, ко второму (канальному) и третьему (сетевому) уровням.

Таблица 6.1 – Основные компоненты стандарта H.323

Рекомендация	Описание
H.225	Определяет сообщения по управлению вызовом, включая сигнализацию и регистрацию, а также пакетизацию и синхронизацию потоков мультимедийных данных

H.245	Определяет сообщения для открытия и закрытия каналов для передачи потоков мультимедийных данных, а также другие команды и запросы
H.261	Видеокодек для аудиовизуальных сервисов на каналах P x 64 кбит/с
H.263	Описывает новый видеокодек для передачи видео по обычным телефонным сетям
G.711	Аудио кодек, 3,1 кГц на 48, 56, и 64 кбит/с
G.722	Аудио кодек, 7 кГц на 48, 56, и 64 кбит/с
G.728	Аудио кодек, 3,1 кГц на 16 кбит/с
G.723	Аудио кодек, для режимов 5,3 и 6,3 кбит/с
G.729	Аудио кодек

Протокол инициирования сеансов связи – SIP

Принципы протокола SIP

За годы работы с протоколом H.323 накоплен большой опыт использования, который позволил выявить как его положительные черты, так и недостатки, которые были учтены при разработке протокола SIP.

Протокол инициирования сеансов – Session Initiation Protocol (SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и передачи данных. Пользователи могут принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи.

Приглашения могут быть адресованы определенному пользователю, группе пользователей или всем пользователям.

Протокол SIP разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543.

В основу протокола рабочая группа MMUSIC заложила следующие принципы:

Персональная мобильность пользователей.

Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения – REGISTER – информирует о своих перемещениях сервер определения местоположения.

Масштабируемость сети.

Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.

Расширяемость протокола.

Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

Расширение функций протокола SIP может быть произведено за счет введения новых заголовков сообщений. При этом, если SIP-сервер принимает сообщения с неизвестными ему полями, то он просто игнорирует их и обрабатывает лишь те поля, которые он знает.

Для расширения возможностей протокола SIP могут быть также добавлены и новые типы сообщений.

Интеграция в стек существующих протоколов Internet, разработанных IETF.

Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом IETF. Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol - RSVP), транспортный протокол реального времени (Real-Time Transport Protocol - RTP), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol - RTSP). Однако функции протокола SIP не зависят ни от одного из этих протоколов.

Взаимодействие с другими протоколами сигнализации.

Протокол SIP может быть использован совместно с протоколом H.323. Возможно даже взаимодействие протокола SIP с системами сигнализации ТфОП – DSS1 и ОКС7. Для упрощения такого взаимодействия сигнальные сообщения протокола SIP могут переносить не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата.

Интеграция протокола SIP с IP-сетями

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. Но, в то же время, предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. При этом, правда, необходимо создать дополнительные механизмы для надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и др.

Здесь же следует отметить то, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки.

Таблица 6.2. Место протокола SIP в стеке протоколов TCP/IP

Протокол инициирования сеансов связи (SIP)	Прикладной уровень
Протоколы TCP и UDP	Транспортный уровень
Протоколы IPv4 и IPv6	Сетевой уровень
PPP, ATM, Ethernet	Уровень звена данных
UTP5, SDH, PDH, V.34 и др	Физический уровень

По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходим механизм обмена информацией о том, какие сервисы может использовать вызываемая\вызывающая стороны. Для этой цели используется протокол SDP (Session Description Protocol) - протокол описания сессии. Данный протокол позволяет определить, какие звуковые (видео и другие) кодеки и иные возможности может использовать удаленная сторона.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP (Real-time Transport Protocol, протокол транспортировки в реальном времени). Таким образом, сам протокол SIP непосредственного участия в передаче голосовых, видео и других данных не принимает, он отвечает только за установление связи (по протоколам SDP, RTP и др.), поэтому под SIP-телефонией понимается не передача голоса по протоколу SIP, а

передача голоса с использованием протокола SIP. Использование протокола SIP предоставляет новые возможности установления соединений (а также возможность беспроблемного расширения данных возможностей), а не непосредственной передачи голосового и других видов трафика.

В глобальной информационной сети Интернет уже довольно давно функционирует экспериментальный участок Mbone, который образован из сетевых узлов, поддерживающих режим многоадресной рассылки мультимедийной информации. Важнейшей функцией Mbone является поддержка мультимедийных конференций, а основным способом приглашения участников к конференции стал протокол SIP. Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, т.е. двусторонний сеанс может перейти в конференцию.

Предназначенный для инициации сеансов протокол SIP обеспечивает определение адреса пользователя и установления соединения с ним. Кроме этого, он служит основой для применения других протоколов, реализующих функции защиты, аутентификации, описания канала мультимедийной связи и т.д.

Адресация

Для организации взаимодействия с существующими приложениями IP-сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций используются специальные универсальные указатели ресурсов - URL (Universal Resource Locators), так называемые SIP URL.

SIP-адреса бывают четырех типов:

• имя@домен;

• имя@хост;

• имя@IP-адрес;

• №телефона@шлюз.

Таким образом, адрес состоит из двух частей. Первая часть - это имя пользователя, зарегистрированного в домене или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.

Во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен - Domain Name Service (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться напрямую.

В начале SIP-адреса ставится слово «sip:», указывающее, что это именно SIP-адрес, т.к. бывают и другие (например, «mailto:»). Ниже приводятся примеры SIP-адресов:

sip: als@rts.loniis.ru

sip: user1@192.168.100.152

sip: 294-75-47@gateway.ru

Архитектура сети SIP

SIP использует обычные текстовые сообщения и очень напоминает HTTP протокол (практически базируется на нем). Архитектура сети SIP базируется на клиент-серверном взаимодействии (рисунок 2.6).

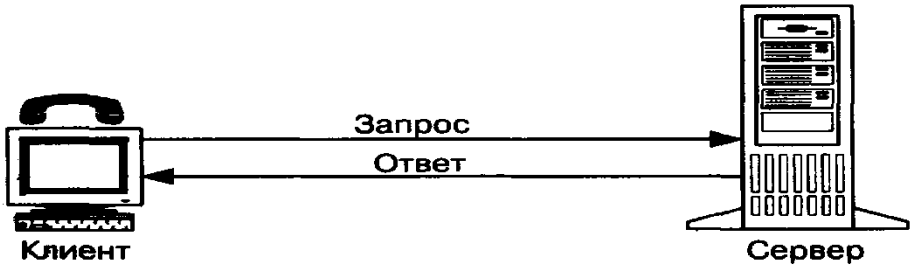


Рис. 6.6. Архитектура "клиент-сервер"

Стандартными элементами в SIP-сети являются:

1. User Agent: по протоколу SIP устанавливаются соединения "клиент-сервер". Клиент устанавливает соединения, а сервер принимает вызовы, но так обычно телефонный аппарат (или программный телефон) может, как устанавливать, так и принимать звонки, то получается, что он одновременно играет роль и клиента и сервера (хотя в реализации протокола это не является обязательным критерием) - в этом случае его называют User Agent (UA) или терминал.

В составе UA выделяются две логические составляющие:

агент-клиент (UAC - user agent client) - посылает запросы и получает ответы;

агент-сервер (UAS - user agent server) - принимает запросы и посылает ответы.

Ввиду того, что большинству устройств необходимо как передавать, так и принимать данные, в реальных устройствах присутствует как UAC, так и UAS.

2. Прокси-сервер: прокси-сервер принимает запросы и производит с ним некоторые действия (например, определяет местоположение клиента, производит переадресацию или перенаправление вызова и др.). Он также может устанавливать собственные соединения. Зачастую прокси-сервер совмещают с сервером определения местоположения (Register-сервер), в таком случае его называют Registrar-сервером.

3. Сервер определения местоположения или сервер регистрации (Register): данный вид сервера служит для регистрации пользователей. Регистрация пользователя производится для определения его текущего IP-адреса, для того чтобы можно было произвести вызов user@IP-адрес. В случае если пользователь переместится в другое место и/или не имеет определенного IP-адреса, его текущий адрес можно будет определить после того, как он зарегистрируется на сервере регистрации. Таким образом, клиент останется доступен по одному и тому же SIP-адресу вне зависимости от того, где на самом деле находится.

4. Сервер переадресации (Redirect): обращается к серверу регистрации для определения текущего IP-адреса пользователя, но в отличие от прокси-сервера только «переадресует» клиента, а не устанавливает собственные соединения.

В результате SIP архитектура выглядит следующим образом (рисунок 6.7):

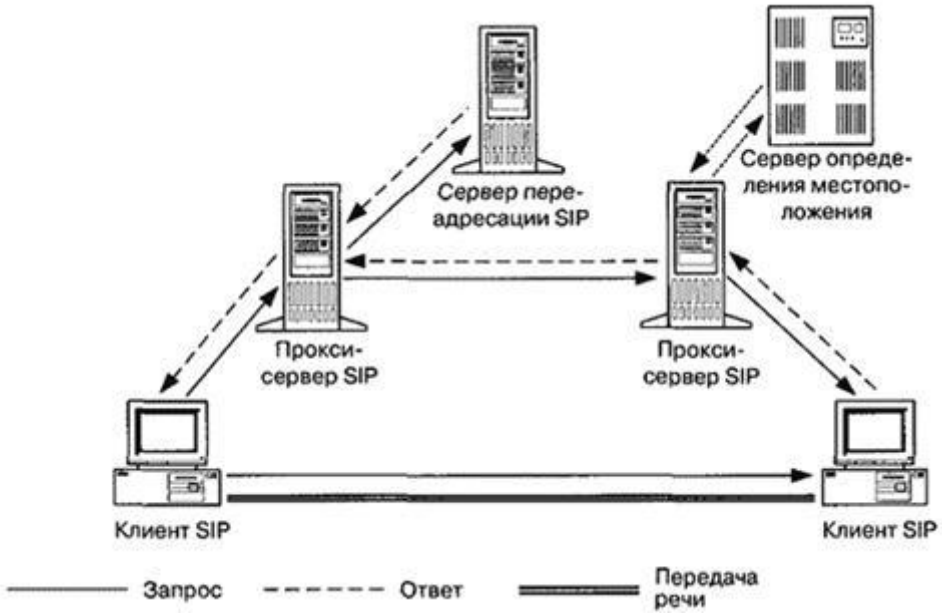


Рис. 6.7. Архитектура сети на базе протокола SIP

Сигнализация на основе протокола SIP

При организации мультимедийного сеанса используется два основных метода для нахождения и информирования заинтересованных участников:

Уведомление о сеансе с использованием разных средств – электронной почты, новостных групп, WEB-страниц или специального протокола SAP (Session Announcement Protocol);

Приглашение к участию в сеансе с помощью протокола SIP.

Ниже приведена на рисунке 6.4 схема сигнализации по протоколу SIP.

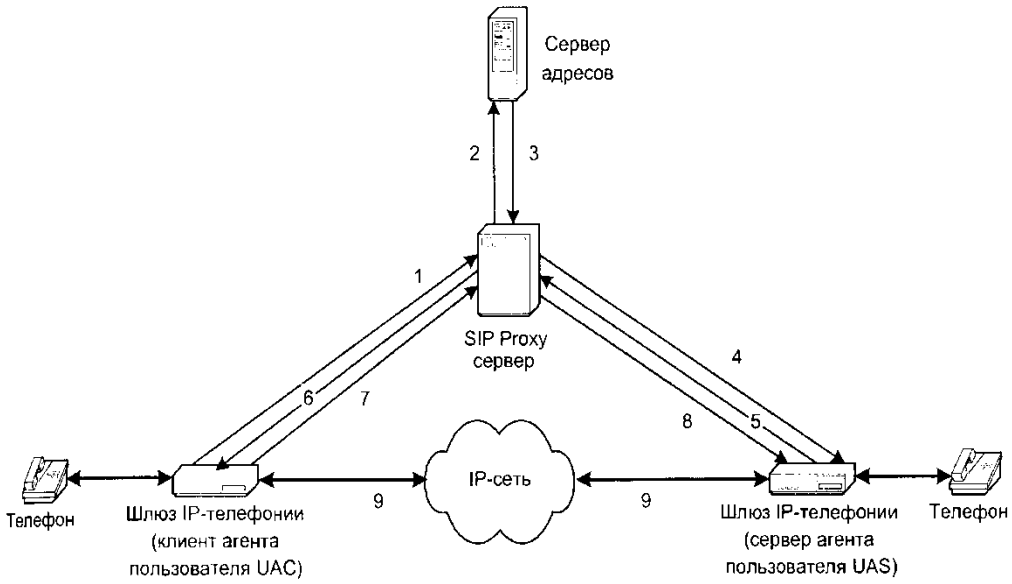


Рис. 6.8. Схема сигнализации по протоколу SIP

1 SIP INVITE; 2 Поиск сервера адресов; 3 Ответ сервера адресов; 4 Пересылка INVITE; 5 Ответ; 6 Пересылка ответа; 7 АСК; 8 Пересылка АСК; 9 Мультимедийный поток

Обработка вызовов осуществляется сервером SIP, который может работать в режиме непосредственного установления связи или в режиме переадресации. В обоих режимах сервер принимает запросы на определение местоположения нужного пользователя, но если в первом режиме он сам доводит вызов до адресата, то во втором – возвращает адрес конечного пункта запрашиваемому клиенту.

В протоколе SIP определены два вида сигнальных сообщений – запрос и ответ.

Они имеют текстовый формат (кодировка символов согласно RFC 2279) и базируются на протоколе HTTP. В запросе указываются процедуры, вызываемые для выполнения требуемых операций, а в ответе – результаты их выполнения. Определены шесть процедур:

INVITE - вызывает адресата для установления связи. С помощью этого сообщения адресату передаются виды поддерживаемых сервисов (которые могут быть использованы инициатором сеанса), а также виды сервисов, которые желает передавать инициатор связи;

ACK - сообщение, подтверждающее согласие адресата установить соединения. В этом сообщении могут быть переданы окончательные параметры сеанса связи (окончательно выбираются виды сервисов и их параметры которые будут использованы);

Cancel – прекращает поиск пользователя;

BYE - запрос завершения соединения;

Register - данным запросом пользователь идентифицирует свое текущее местоположение;

OPTIONS - запрос информации о функциональных возможностях терминала (применяется в случае, если эти данные нужно получить до установления соединения, то есть до фактического обмена данной информацией с помощью запросов INVITE и ACK).

Предназначенный для инициации сеансов протокол SIP обеспечивает определение адреса пользователя и установление соединения с ним. Кроме этого, он служит основой для применения других протоколов, реализующих функции защиты, аутентификации, описания канала мультимедийной связи и т.д.

Обеспечение качества IP-телефонии

Показатели качества IP-телефонии

Традиционные телефонные сети коммутируют электрические сигналы с гарантированной полосой пропускания, достаточной для передачи сигналов голосового спектра. При фиксированной пропускной способности передаваемого сигнала цена единицы времени связи зависит от удаленности и расположения точек вызова и места ответа.

Сети с коммутацией пакетов не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированного пути между точками связи.

IP-телефония является одной из областей передачи данных, где важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации, а также увеличением пропускной способности каналов, что приводит к возможности успешной конкуренции IP-телефонии с традиционными телефонными сетями.

Основными составляющими качества IP-телефонии являются:

Качество речи, которое включает:

- диалог – возможность пользователя связываться и разговаривать с другим пользователем в реальном времени и полнодуплексном режиме;

- разборчивость – чистота и тональность речи;

- эхо – слышимость собственной речи;

- уровень – громкость речи.

Качество сигнализации, включающее:

- установление вызова – скорость успешного доступа и время установления соединения;

- завершение вызова – время отбоя и скорость разъединения;

- DTMF – определение и фиксация сигналов многочастотного набора номера.

Факторы, которые влияют на качество IP-телефонии, могут быть разделены на две категории:

Факторы качества IP- сети:

- максимальная пропускная способность – максимальное количество полезных и избыточных данных, которая она передает;

- задержка – промежуток времени, требуемый для передачи пакета через сеть;

- джиттер - задержка между двумя последовательными пакетами;

- потеря пакета – пакеты или данные, потерянные при передачи через сеть.

Факторы качества шлюза:

- требуемая полоса пропускания - различные кодеки требуют различную полосу. Например, кодек G.723 требует полосы 16,3 кбит/с для каждого речевого канала;

- задержка - время, необходимое цифровому сигнальному процессору DSP или другим устройствам обработки для кодирования и декодирования речевого сигнала;

- буфер джиттера - сохранение пакетов данных до тех пор, пока все пакеты не будут получены, и можно будет передать в требуемой последовательности для минимизации джиттера;

- потеря пакетов - потеря пакетов при сжатии и/или передаче в оборудовании IP-телефонии;

подавление эхо — механизм для подавления эхо, возникающего при передаче по сети;

- управление уровнем - возможность регулировать громкость речи.

Влияние сети на показатели качества IP-телефонии

Задержка

Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эхо. Эхо возникает в случае, когда отраженный речевой сигнал вместе с сигналом от удаленного конца возвращается опять в ухо говорящего. Эхо становится трудной проблемой, когда задержка в петле передачи больше, чем 50 мс. Так как эхо является проблемой качества, системы с пакетной коммутацией речи должны иметь возможность управлять эхо и использовать эффективные методы эхоподавления.

Затруднение диалога и перекрытие разговоров становятся серьезным вопросом качества, когда задержка в одном направлении передачи превышает 250 мс. Можно выделить следующие источники задержки при пакетной передаче речи из конца в конец [1].

Задержка накопления (иногда называется алгоритмической задержкой): эта задержка обусловлена необходимостью сбора кадра речевых отсчетов, выполняемая в речевом кодере. Величина задержки определяется типом речевого кодера и изменяется от небольших величин (0,125 мкс) до нескольких миллисекунд. Например, стандартные речевые кодеры имеют следующие длительности кадров:

G.729 CS-ACELP (8 кбит/с) – 10 мс

G.723.1 – Multi Rate Coder (5,3; 6,3 кбит/с) – 30 мс.

Задержка обработки: процесс кодирования и сбора закодированных отсчетов в пакеты для передачи через пакетную сеть создает определенные задержки. Задержка кодирования или

обработки зависит от времени работы процессора и используемого типа алгоритма обработки.

Сетевая задержка: задержка обусловлена физической средой и протоколами, используемыми для передачи речевых данных, а также буферами, используемыми для удаления джиттера пакетов на приемном конце. Сетевая задержка зависит от емкости сети и процессов передачи пакетов в сети.

Время задержки при передачи речевого сигнала можно отнести к одному из трех уровней:

первый уровень до 200 мс – отличное качество связи. Для сравнения, в телефонной сети общего пользования допустимы задержки до 150-200 мс;

второй уровень до 400 мс – считается хорошим качеством связи. Но если сравнивать с качеством связи по сетям ТФОП, то разница будет видна. Если задержка постоянно удерживается на верхней границе 2-го уровня (на 400 мс), то не рекомендуется использовать эту связь для деловых переговоров;

третий уровень до 700 мс – считается приемлемым качеством связи для ведения неделовых переговоров. Такое качество связи возможно также при передаче пакетов по спутниковой связи.

Качество Интернет-телефонии попадает под 2-3 уровни, провайдеры IP-телефонии, работающие по выделенным каналам попадают под 1-2 уровни. Также необходимо учитывать задержки при кодировании/декодировании голосового сигнала. Средние суммарные задержки при использовании IP-телефонии обычно находятся в пределах 150-250 мс.

Джиттер

Когда речь или данные разбиваются на пакеты для передачи речи через IP-сеть, пакеты часто прибывают в пункт назначения в различное время и в разной последовательности. Это создает разброс времени доставки пакетов (джиттер). Джиттер приводит к специфическим нарушениям передачи речи, слышимым как трески и щелчки.

Для того, чтобы компенсировать влияние джиттера, в терминалах используется так называемый джиттер-буфер. Этот буфер хранит в памяти прибывшие пакеты в течение времени, определяемого ее емкостью (длиной). Пакеты, прибывшие слишком поздно, когда буфер заполнен, отбрасываются. Интервалы между пакетами восстанавливаются на основе значений временных меток RTP-пакетов. В функции джиттер-буфера входит и восстановление исходной очередности следования пакетов, если при транспортировки по сети они оказались «перепутаны».

Слишком короткий буфер будет приводить к слишком частым потерям «опоздавших» пакетов, а слишком длинный – к неприемлемо большой дополнительной задержке. Обычно

предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения.

Для оптимизации джиттер-буфера в VoIP-устройстве следует повышать размер буфера, что позволяет снижать или вообще устранять джиттер, размер буфера, превышающий 150 мс, достаточно сильно влияет на качество разговора.

Потеря пакетов

Потерянные пакеты в IP-телефонии нарушают речь и создают искажения тембра. В существующих IP-сетях все голосовые данные. При пиковых нагрузках и перегрузках голосовые кадры будут отбрасываться, как и кадры данных. Однако кадры данных не связаны со временем, и отброшенные пакеты могут быть успешно переданы путем повторения. Потеря голосовых пакетов, в свою очередь, не может быть восполнена таким способом и в результате произойдет неполная передача информации. Предполагается, что потеря до 5% пакетов незаметна, а свыше 10-15% - недопустима. Причем данные величины существенно зависят от алгоритмов компрессии/декомпрессии.

Существенно, что потеря большой группы пакетов приводит к необратимым локальным искажениям речи, тогда как потери одного, двух, трех пакетов можно пытаться компенсировать.

Взаимосвязь методов обеспечения качества IP-телефонии, показателей качества сети и качества вызова представлена на рисунке 6.9.

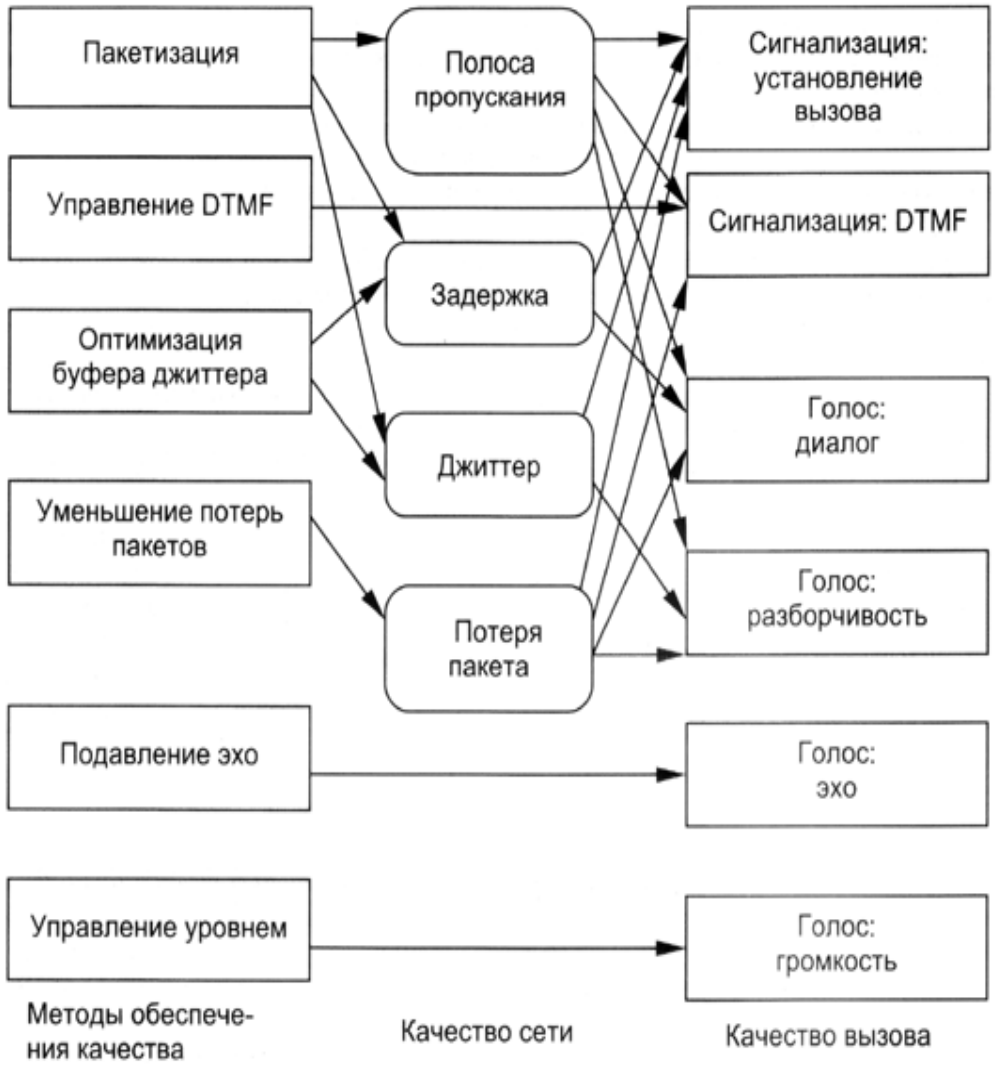


Рис. 6.9. Схема обеспечения качества IP-телефонии

Asterisk

Asterisk — свободное решение компьютерной телефонии (в том числе, VoIP) с открытым исходным кодом от компании Digium, первоначально разработанное Марком Спенсером. Приложение работает на операционных системах Linux, FreeBSD, OpenBSD и Solaris. Имя проекта произошло от названия символа «*» (англ. asterisk — «звездочка»).

Asterisk в комплексе с необходимым оборудованием обладает всеми возможностями классической АТС, поддерживает множество VoIP-протоколов и предоставляет богатые функции управления звонками, среди них:

Голосовая почта.

Конференции.

Интерактивное голосовое меню (IVR).

Центр обработки вызовов (постановка звонков в очередь и распределение их по агентам используя различные алгоритмы).

Запись (Call Detail Record).

Для создания дополнительной функциональности можно воспользоваться собственным языком Asterisk для написания плана нумерации, написав модуль на языке Си, либо воспользовавшись AGI — гибким и универсальным интерфейсом для интеграции с внешними системами обработки данных. Модули, выполняющиеся через AGI, могут быть написаны на любом языке программирования.

Asterisk распространяется на условиях двойной лицензии, благодаря которой одновременно с основным кодом, распространяемым по открытой лицензии GNU GPL, возможно создание закрытых модулей, содержащих лицензируемый код.

Asterisk может работать как с аналоговыми линиями (FXO/FXS модули), так и цифровыми (ISDN, BRI и PRI — потоки T1/E1). С помощью определённых компьютерных плат (наиболее известными производителями которых являются Digium, Sangoma, OpenVox, Rhino, AudioCodes) Asterisk можно подключить к высокопропускным линиям T1/E1, которые позволяют работать параллельно с десятками и сотнями телефонных соединений. Полный список поддерживаемого оборудования для соединения с телефонной сетью общего пользования определяется поддержкой оборудования в модулях ядра.

Для создания дополнительной функциональности можно воспользоваться собственным языком Asterisk для написания плана нумерации, написав модуль на языке C, либо воспользовавшись AGI - гибким и универсальным интерфейсом для интеграции с внешними системами обработки данных. Модули, выполняющееся через AGI, могут быть написаны на любом языке программирования.

Asterisk распространяется на условиях двойной лицензии, благодаря которой одновременно с основным кодом, распространяемым по открытой лицензии GNU GPL, возможно создание закрытых модулей, содержащих лицензируемый код: например, модуль для поддержки кодека G.729.

Благодаря свободной лицензии Asterisk активно развивается и поддерживается тысячами людей со всей планеты. В течение последних двух лет рынок Asterisk-приложений активно развиваются в США и уже заняли прочное место на рынке IT-технологий (более 1000 компаний, центры поддержки, online-консультации). В Россию данный продукт попал позже, но интерес российского потребителя растёт, и в первую очередь, благодаря открытости системы. Многие компании применяют Asterisk в своих серийных VoIP-устройствах, например компании Linksys, Nateks.

Поддерживаются следующие протоколы:

SIP,

H.323,

IAX2,

MGCP,

Skinny/SCCP,

XMPP (Google Talk),

Unistim,

Skype, через коммерческий канал.

Настройка и программирование производится с помощью нескольких механизмов:

диалплан, который пишется на специальном языке. Доступна как старая версия, так и новая — AEL, а также на языке Lua.

AGI.

AMI.

Конфигурация из баз данных.

IP-АТС на основе Asterisk обладает возможностями:

Запись телефонных разговоров

Конференц-комнаты с использованием виртуальных номеров

Голосовая почта и пересылка на e-mail

Поддержка протоколов SIP, IAX2, H.323, MGCP, Skinny

Инструменты разработчика для создания расширений, предоставляющие новые услуги

Поддержка кодеков: ADPCM, G.711 (A-Law и μ-Law), G.722, G.723.1, G.726, G.728, G.729, GSM, ILBC, Speex.

Виртуальный секретарь - IVR

Поддержка аналоговых интерфейсов FXS / FXO

Голосовой синтез речи

Поддержка цифровых интерфейсов (E1/T1/J1) и протоколов PRI/BRI/R2/SS7

Автоконфигурация IP-телефонов

АОН определитель номера

Программное эхоподавление

Работа с несколькими операторами связи

Маршрутизация входящих и исходящих вызовов по различным правилам

Поддержка Видеотелефонов

Интерфейс обнаружения телефонного оборудования

Поддержка групповой переадресации вызовов

DHCP сервер для распределения динамических IP адресов

Панель оператора. Оператор может видеть всю телефонную деятельность в виде графиков и выполнять простые операции по управлению телефонными звонками

Поддержка протокола пейджинга (intercom) и домофонов

Веб-панель управления

Поддержка временных условиях

Парковка и перехват звонка

Запрет вызова по PIN коду

Call Detail Record (CDR) отчеты

Прямой доступ в систему (DISA)

Биллинг, отчеты, статистика, анализ по использованию

Поддержка обратного звонка

Поддержка динамических очередей

Структурная схема IP АТС на базе Asterisk

Asterisk, благодаря гибкой системе настроек, позволяет строить различные решения голосовой связи, в зависимости от требований.

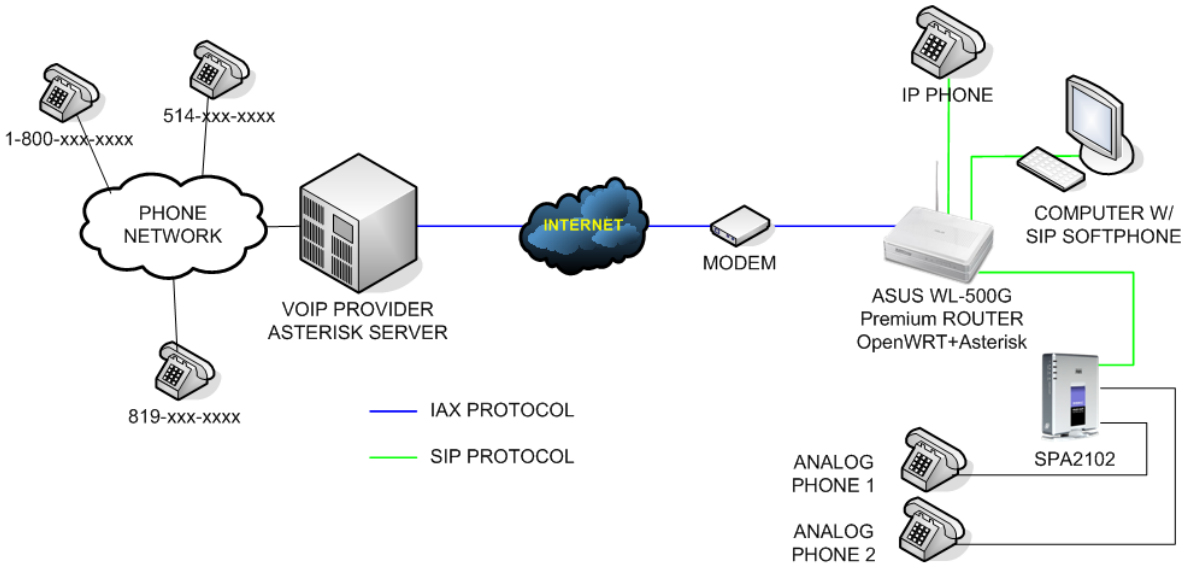


Рис. 6.10. структурная схема сетевого решения на базе Asterisk

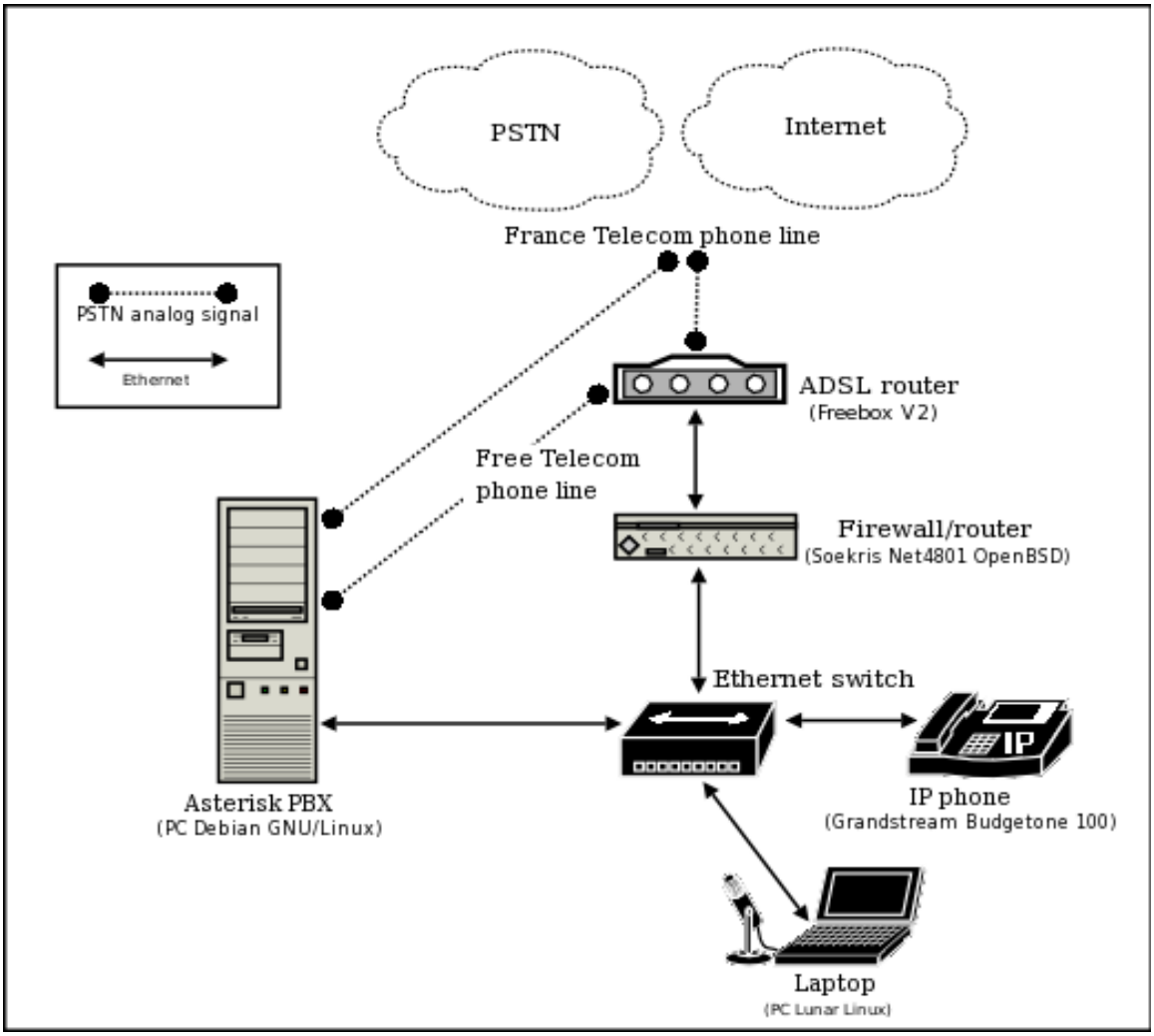
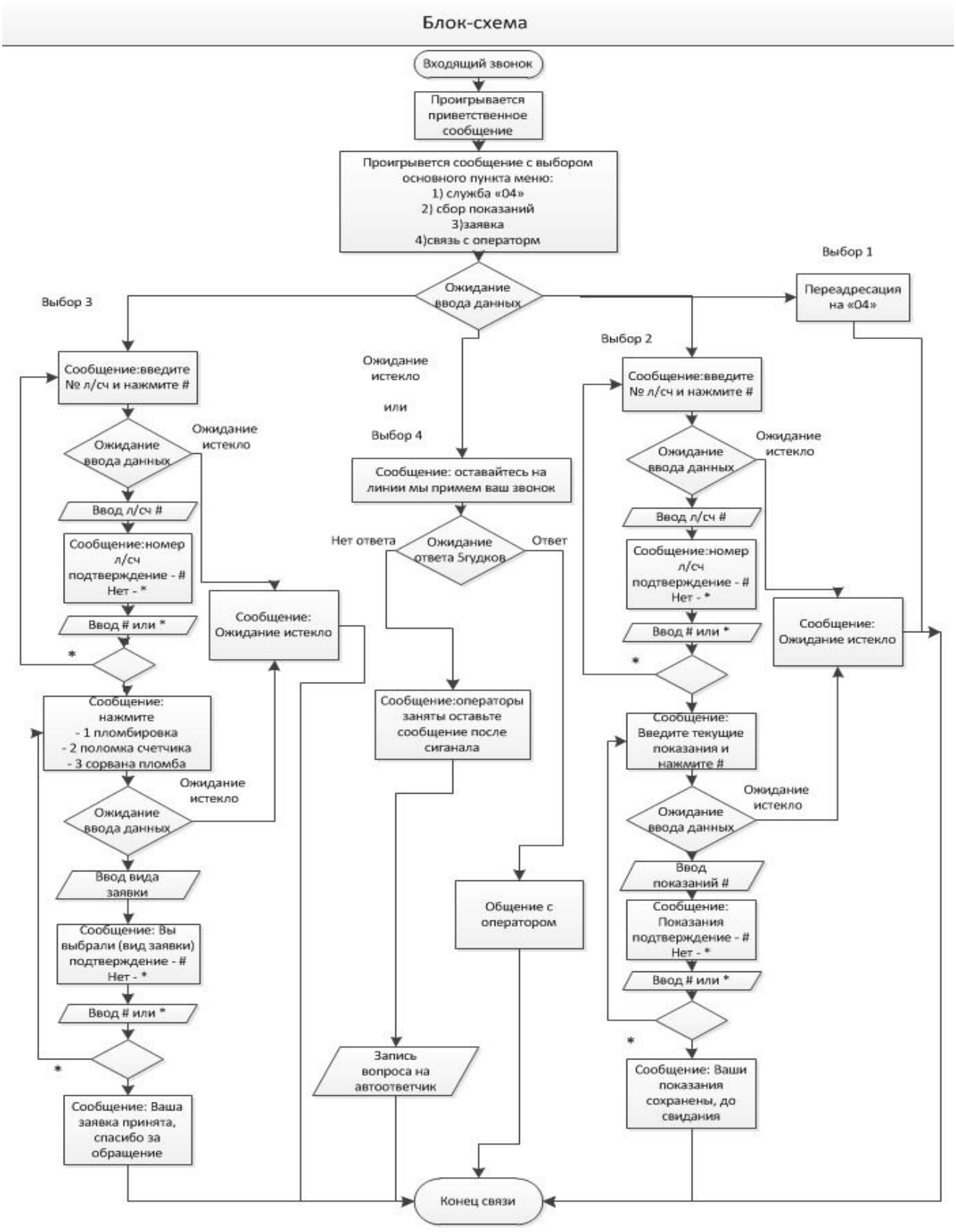


Рис. 6.11. Структурная схема сетевого решения на базе Asterisk

Блок-схема IP-АТС на базе Asterisk. Блок схема алгоритма IP АТС представнена ниже

В процессе проектирования были рассмотрены основные принципы построения сетей IP-



телефонии, выполнена оценка уровня качества разрабатываемой системы. Был произведен выбор, и сравнительный анализ основных протоколов, на базе которых реализована сеть IP-

телефонии, произведен выбор необходимого оборудования, построена структурная схема сети, функциональная схема, а так же блок схема алгоритма защиты сети IP-телефонии.

Компьютерный практикум

Методические указания по настройке системы

Поскольку требования, предъявляемые Asterisk к производительности, главным образом, обусловлены большим объемом производимых математических вычислений, естественным будет выбор процессора с мощным FPU. Выведем рекомендуемые технические характеристики сервера в таблицу 6.3.

Таблица 6.3. Рекомендации по выбору технических характеристик системы

Назначение	Количество каналов	Рекомендуемые параметры
Любительская система	Не более 5	400 МГц x86, 256 М6 оперативной памяти
SOHO-система (малый офис)	От 5 до 10	1 ГГц x86, 512 М6 оперативной памяти
Малая бизнес-система	До 25	3 ГГц x86, 1 Гб операт-й памяти

Все ниже написанное было протестировано на операционных системах Windows 7 и Windows 2008.

Шаг 1

Скачайте и установите asteriskwin32 version 0.66b. Линк: http://www.asteriskwin32.com/.

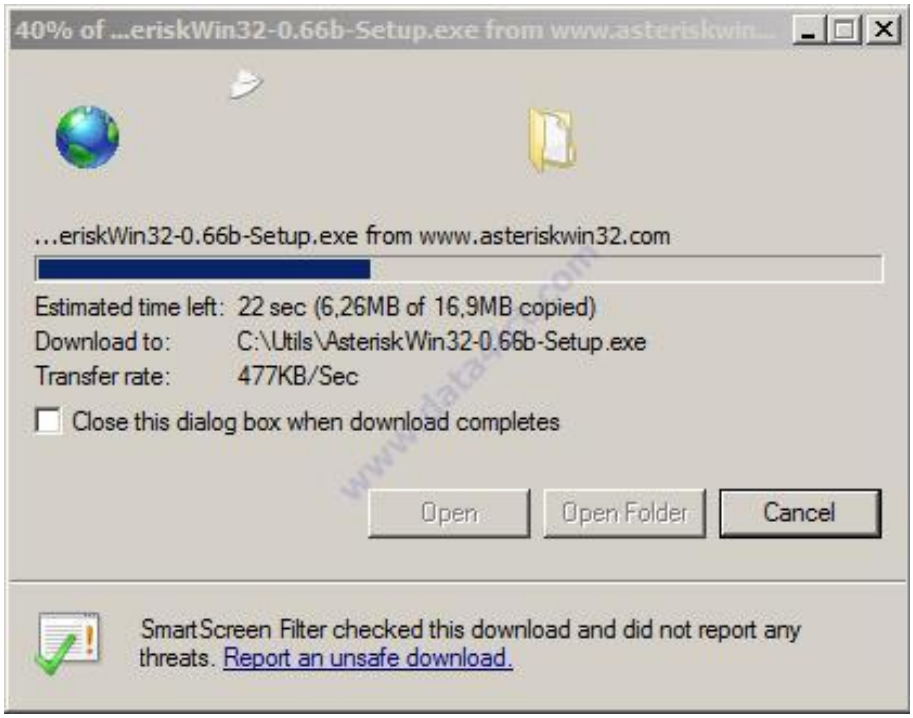


Рис. 6.13. Скачка ПО AsteriskWin32

Шаг 2

Установка скачанного файла начнется после двойного клика по файлу «AsteriskWin32-0.66b-Setup»

Рисунок 6.14. Установка AsteriskWin32

Выберите I accept the agreement

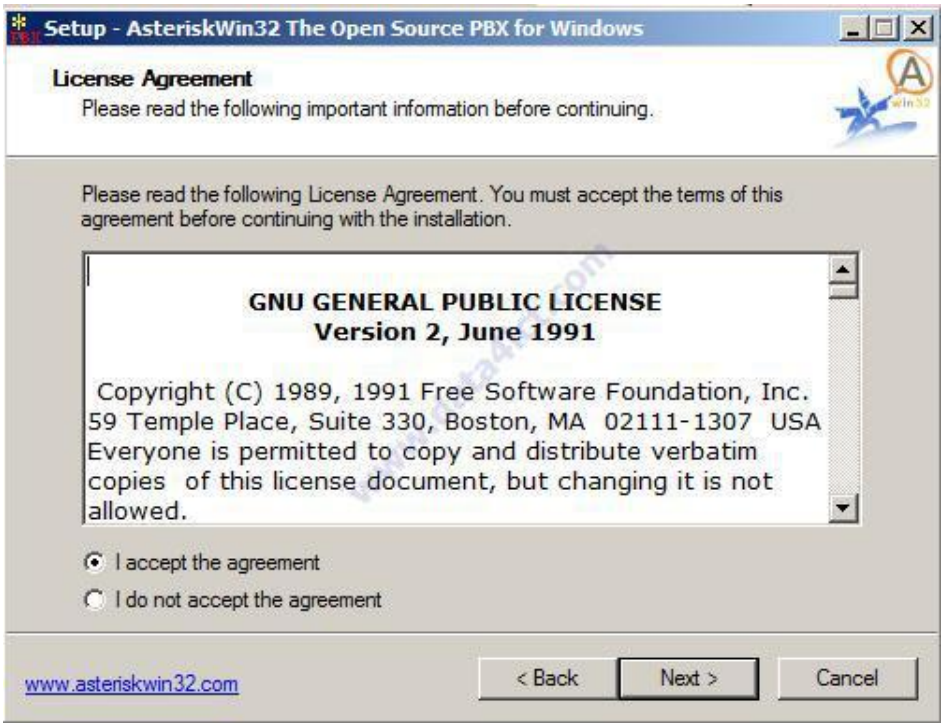


Рис. 6.15. Установка AsteriskWin32

Нажмите next

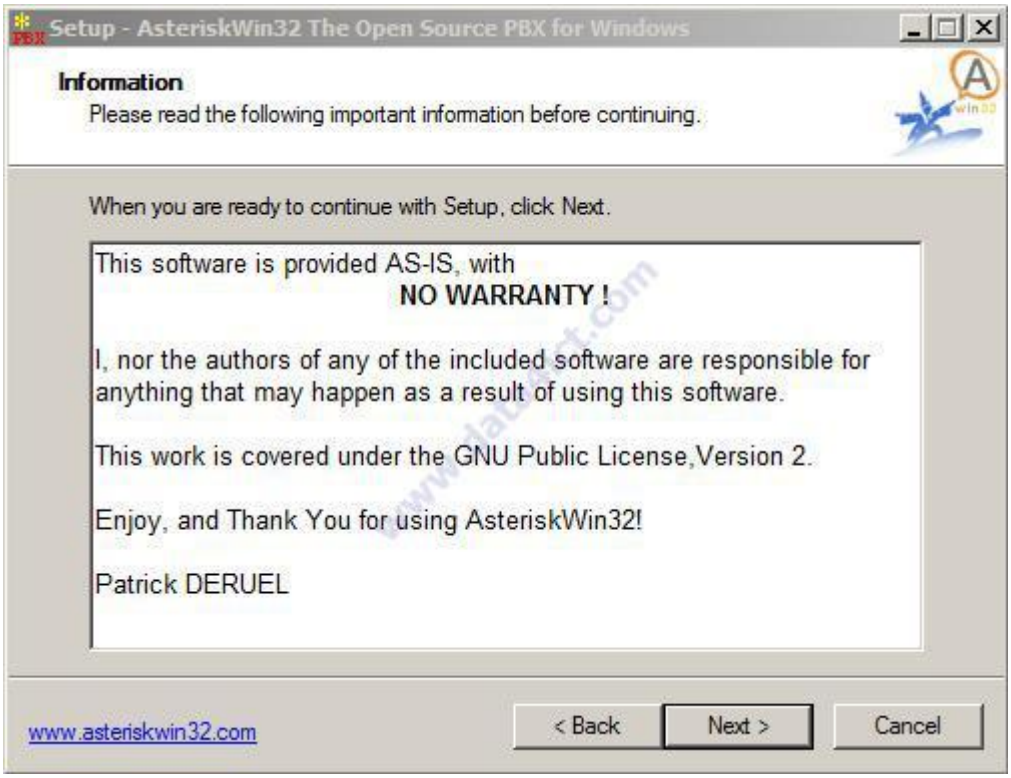


Рис. 6.16. Установка AsteriskWin32

Выберите директорию установки программы, рекомендуется устанавливать в папку cygroot

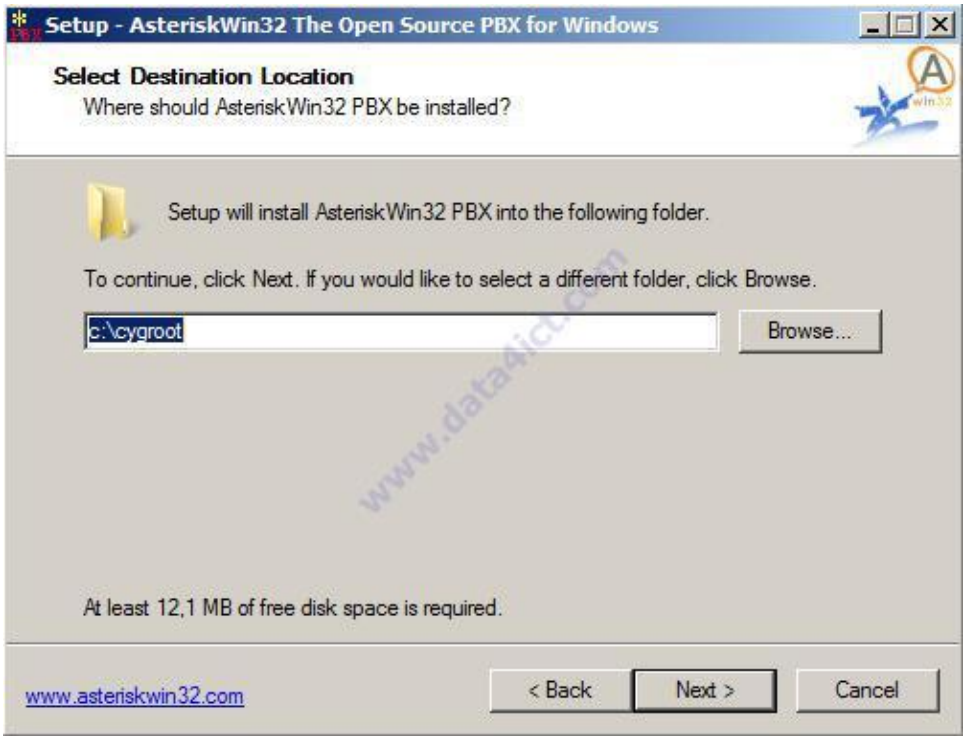


Рис. 6.17. Установка AsteriskWin32

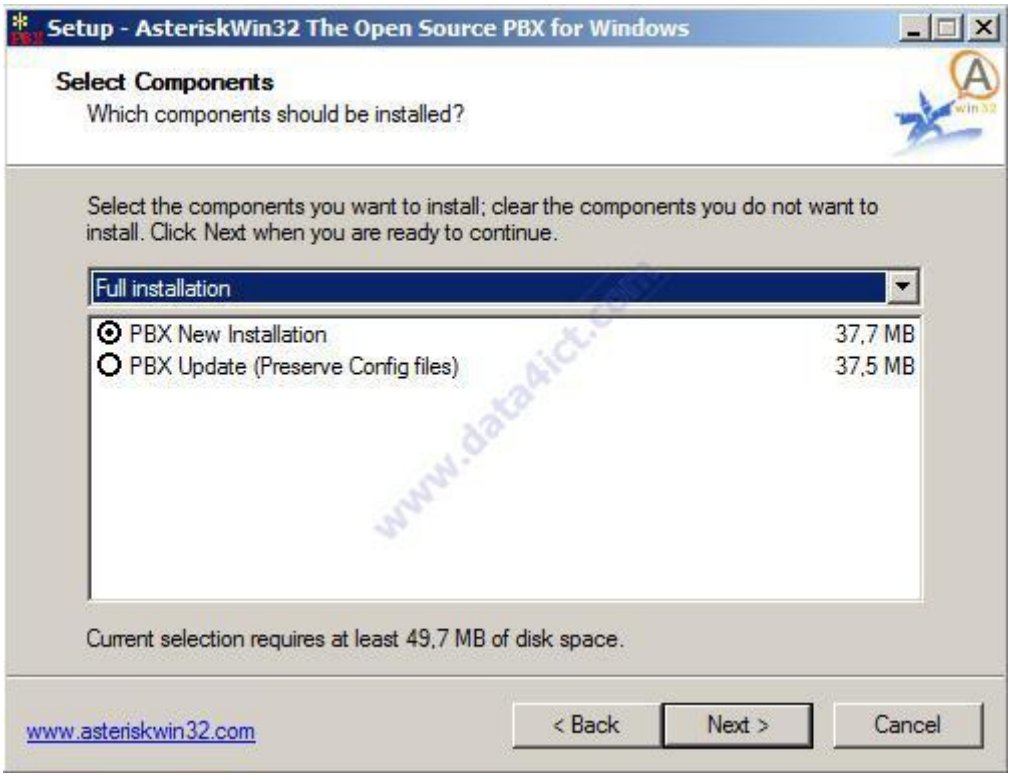


Рис. 6.18. Установка AsteriskWin32

Клик Install

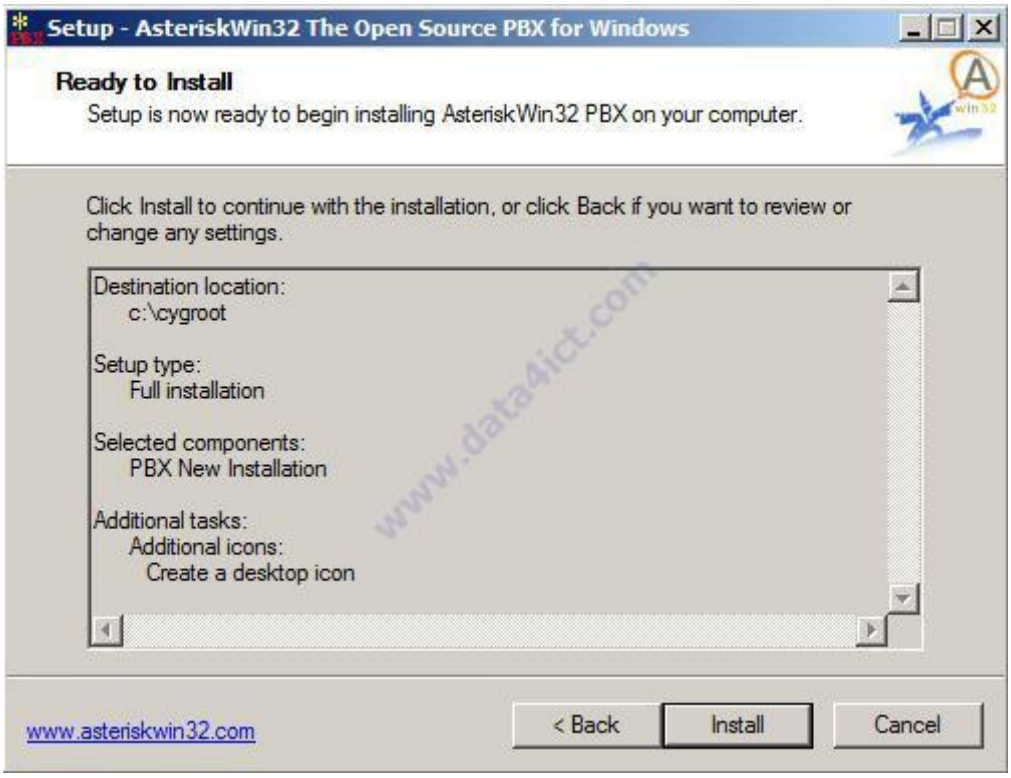


Рис. 6.19. Установка AsteriskWin32

Ждите пока полностью не установится

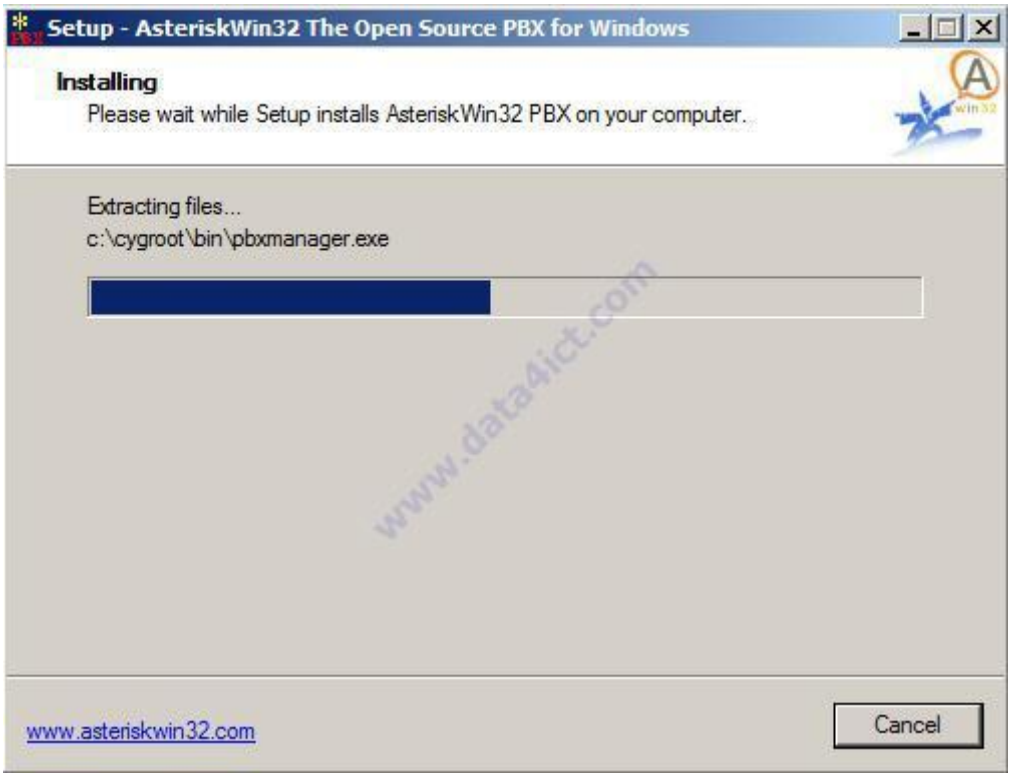


Рис. 6.20. Установка AsteriskWin32

Рис. 6.21. Установка AsteriskWin32

Поздравляю, установка AsteriskWin32 завершена.

Запуск AsteriskWin32

Начните работу Asterisk, дважды кликнув по иконке AsteriskW32 GUI

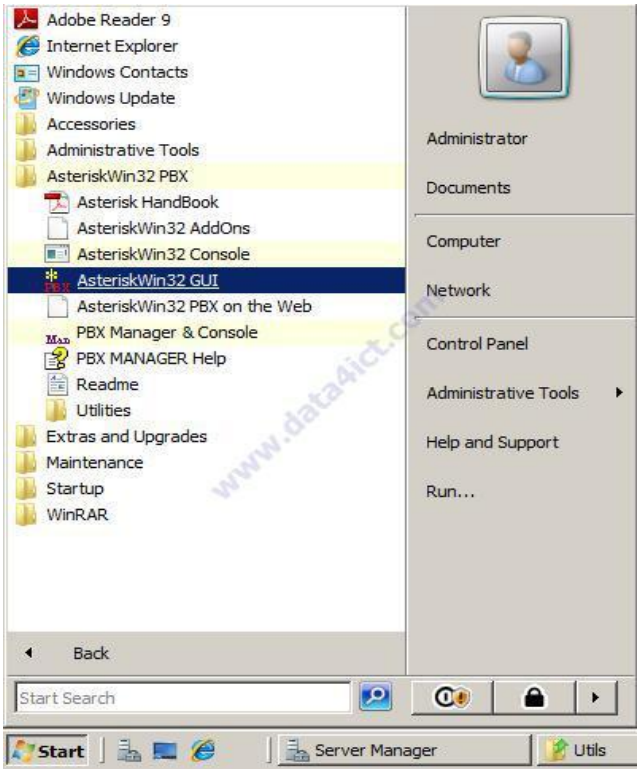


Рис. 6.22. Запуск AsteriskWin32

После запуска программы в командном окне появится несколько ошибок, которые не дадут к корректной работе системы.

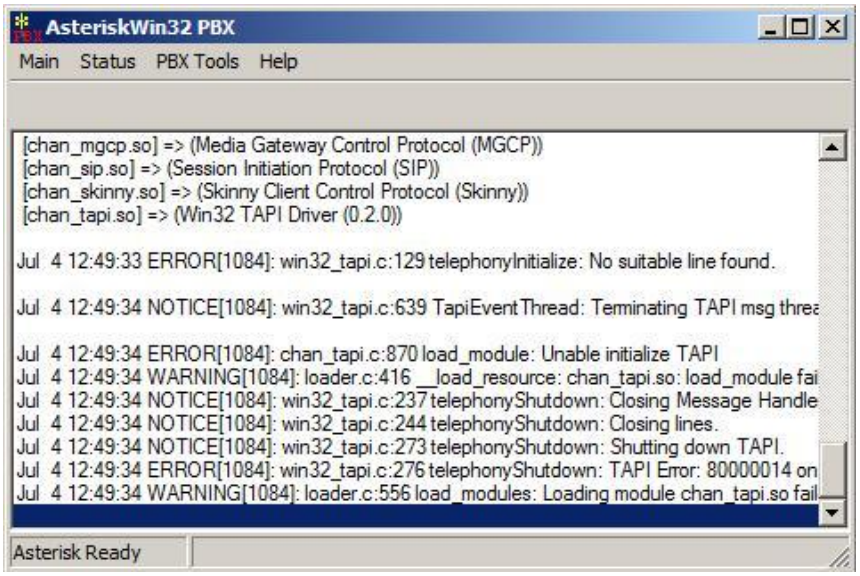


Рис. 6.23. Запуск AsteriskWin32

Для решения данной проблемы, мы скачиваем эмулятор Linux Emulator (cygwin) по линку http://www.cygwin.com/. В пособие рассматривается установка cygwin version 1.7.5.

Устанавливаем скачанный файл

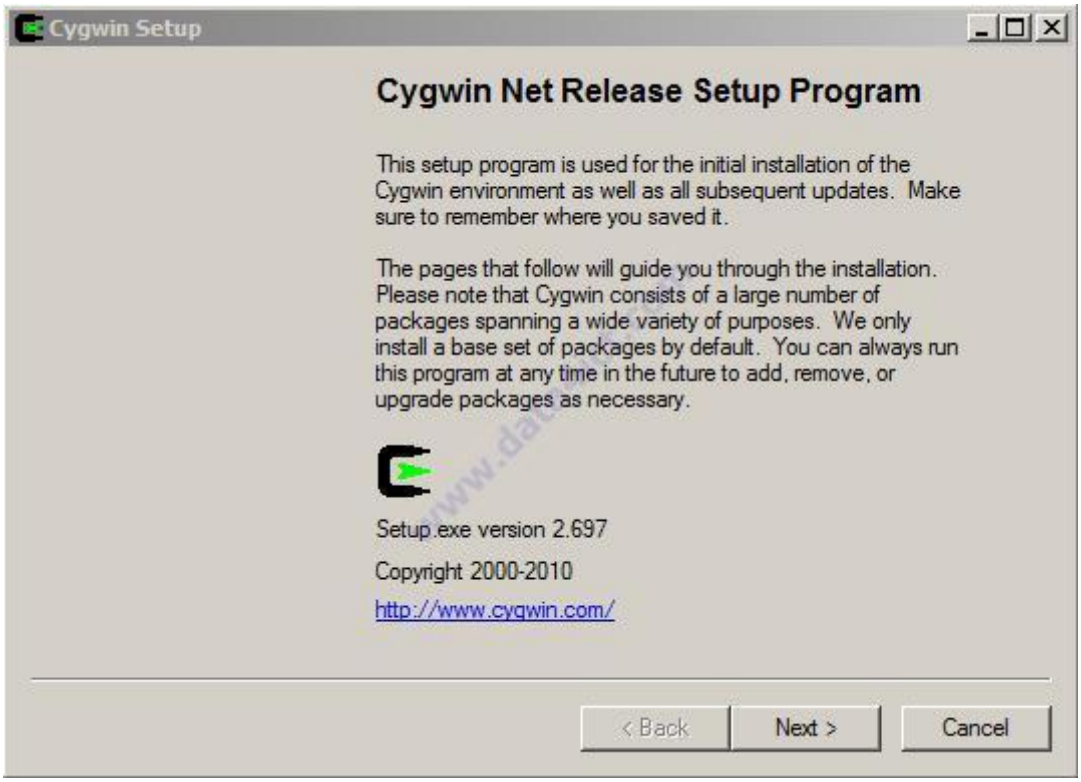


Рис. 6.24. Установка cygwin

Выберем Install from Internet

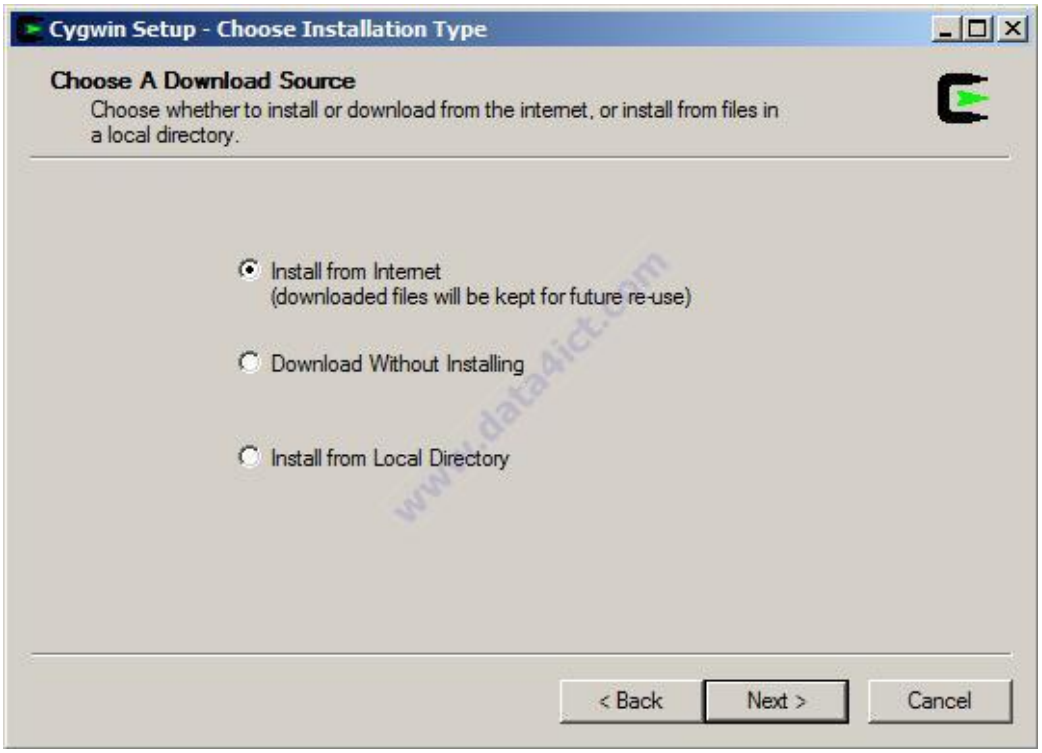


Рис. 6.25. Установка cygwin

Изменяем директорию установки на C:\cygroot и нажинаем Next.

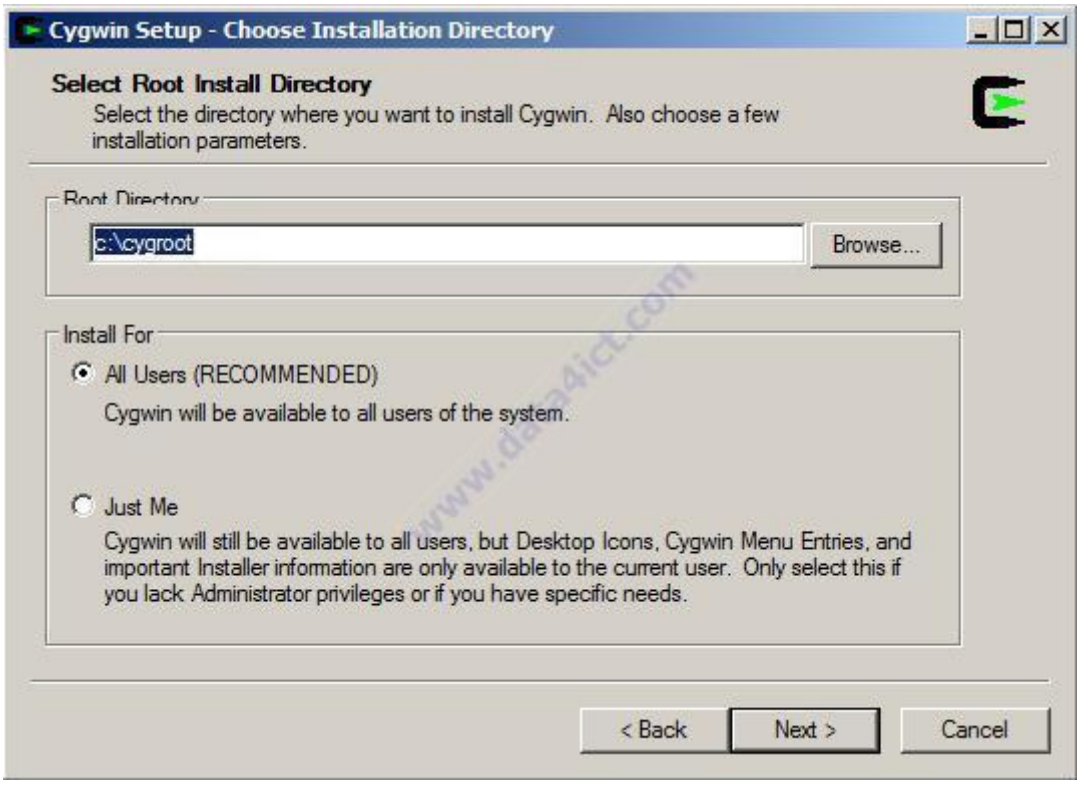


Рис. 6.26. Установка cygwin

Изменяем на C:\Utils

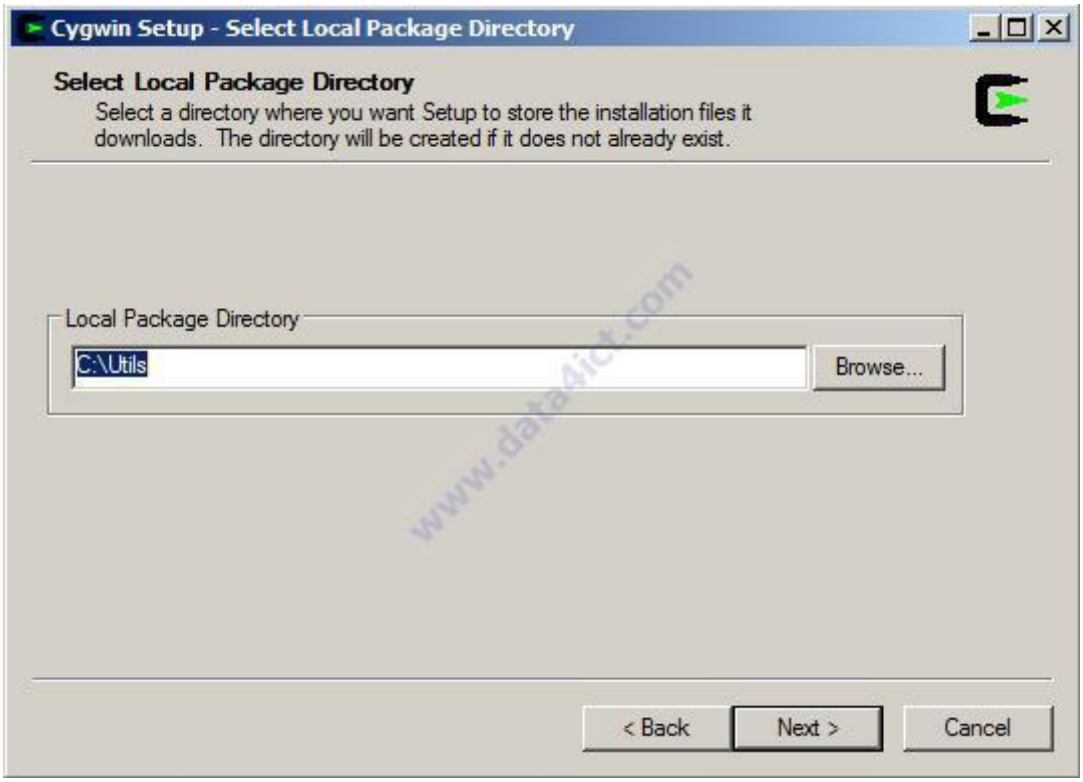


Рис. 6.27. Установка cygwin

Выбираем Direct connection

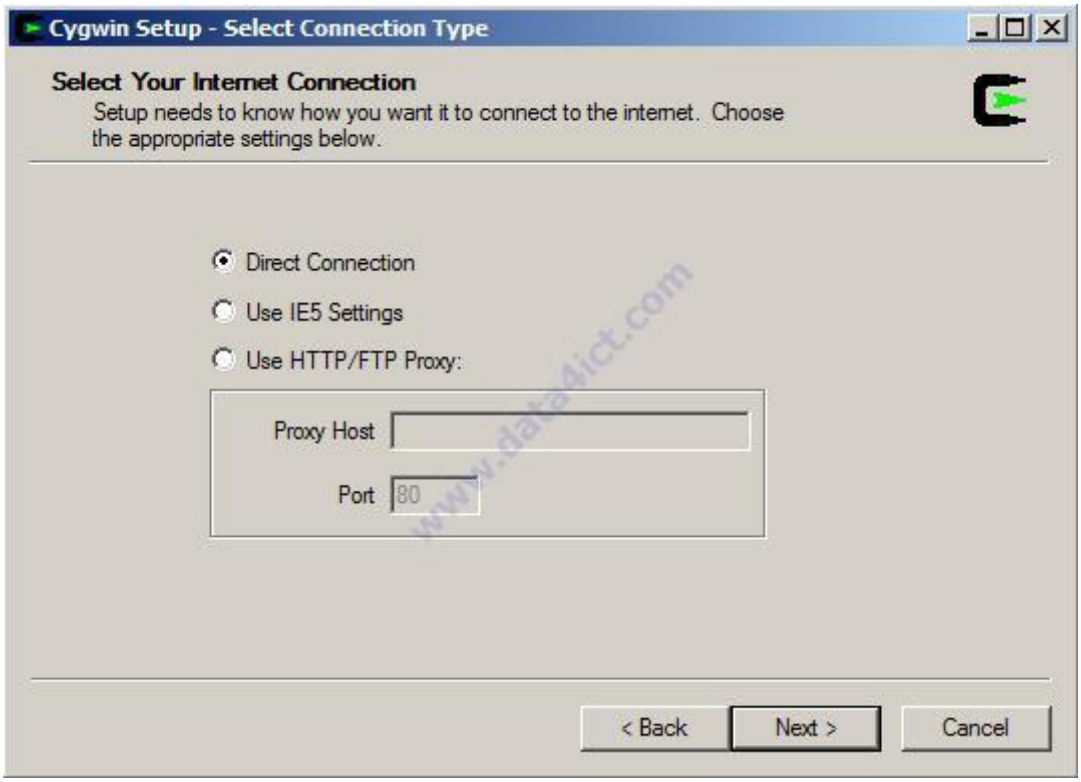


Рис. 6.28. Установка cygwin

Выбираем сайт, с которого будет идти скачивание

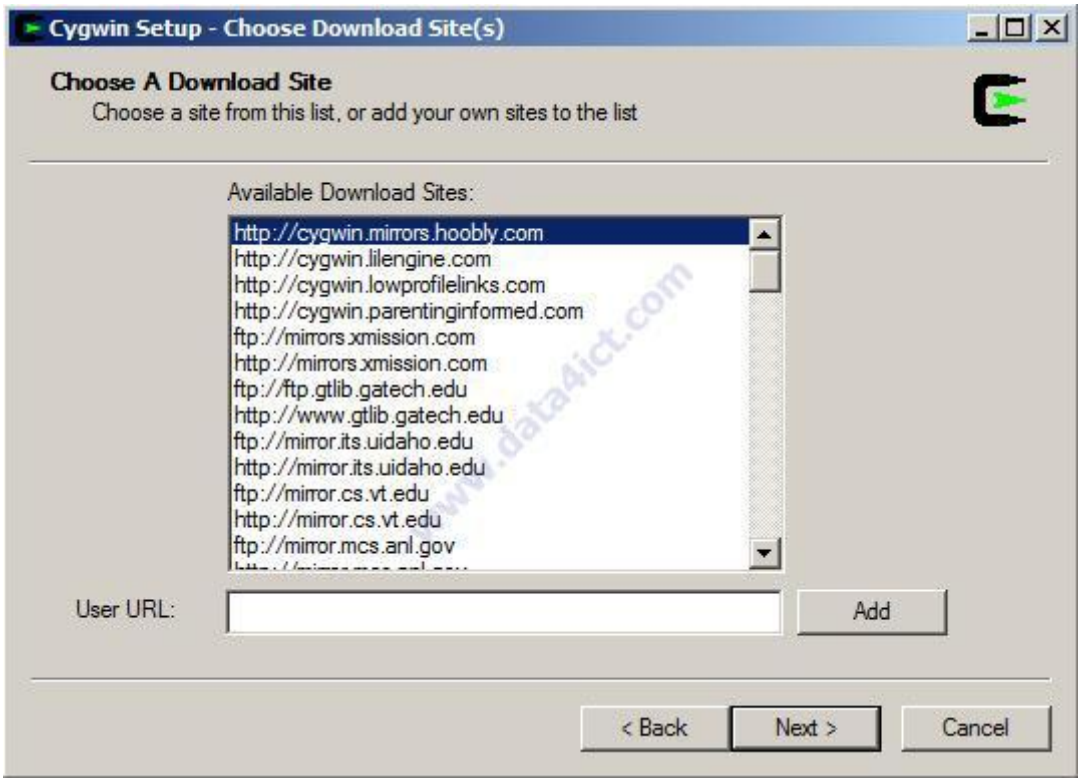


Рис. 6.29. Установка cygwin

Дождитесь до полной скачки файлов

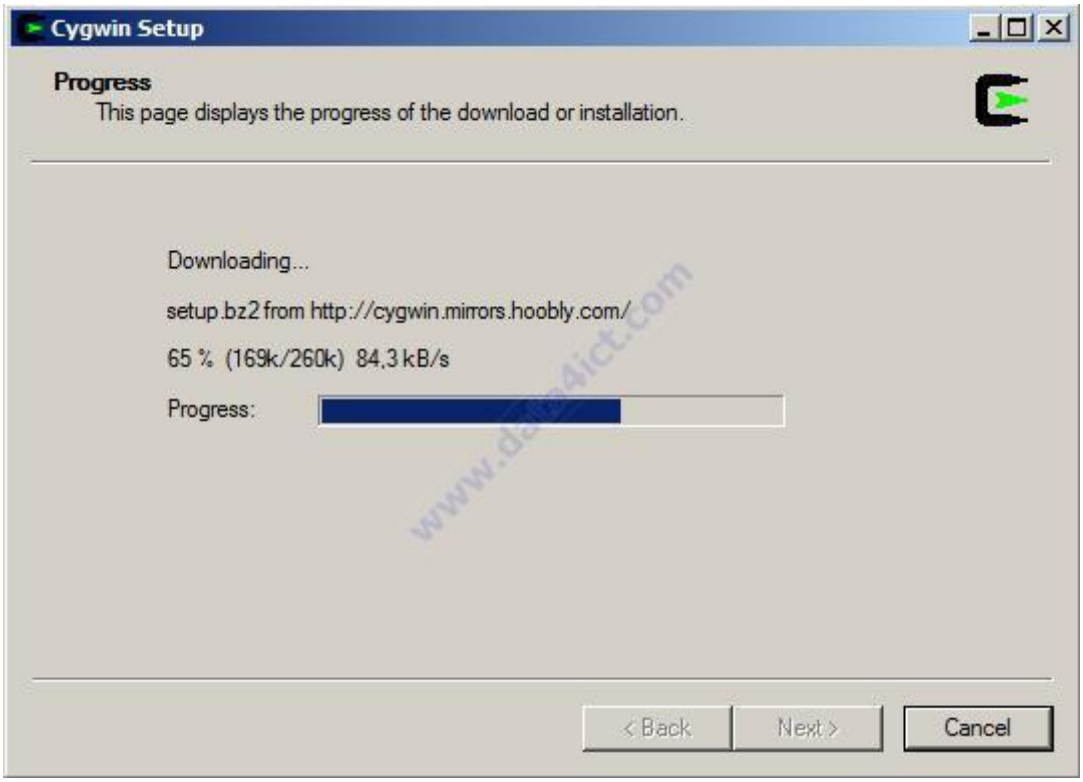


Рисунок 6.30. Установка cygwin

При выскакивании ошибки нажмите Ок

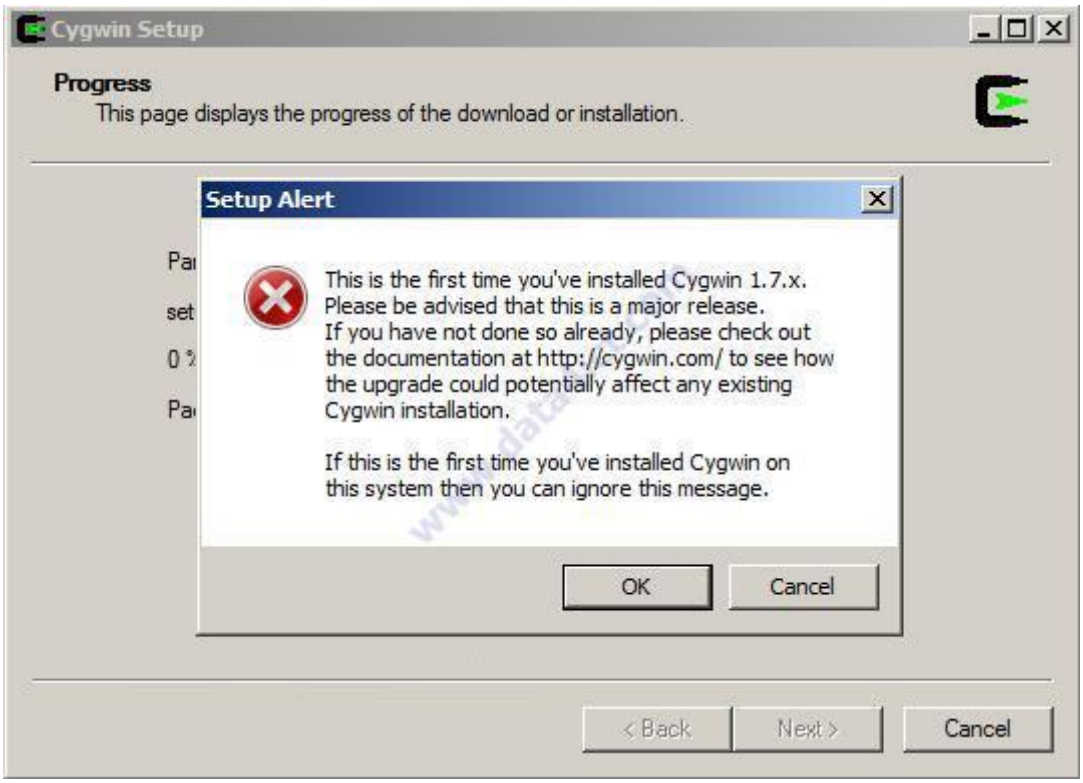


Рис. 6.31. Установка cygwin

Нажмите next

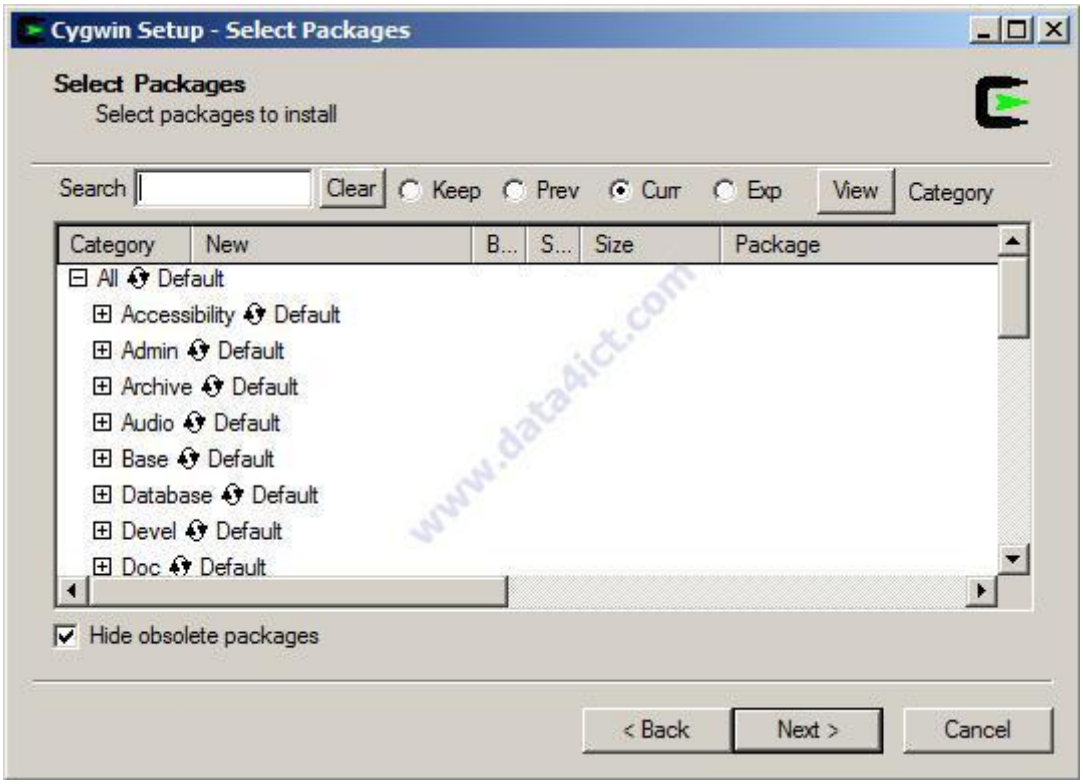


Рис. 6.32. Установка cygwin

Дождитесь полного скачивания

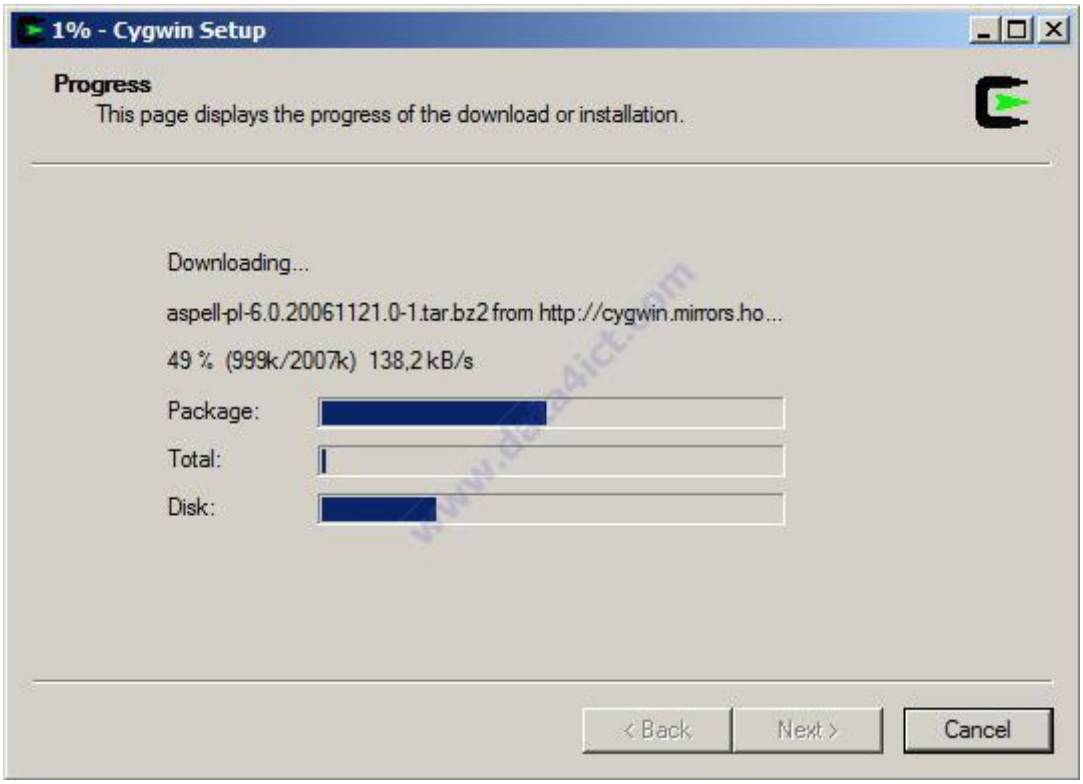


Рис. 6.33. Установка cygwin

Клик finish

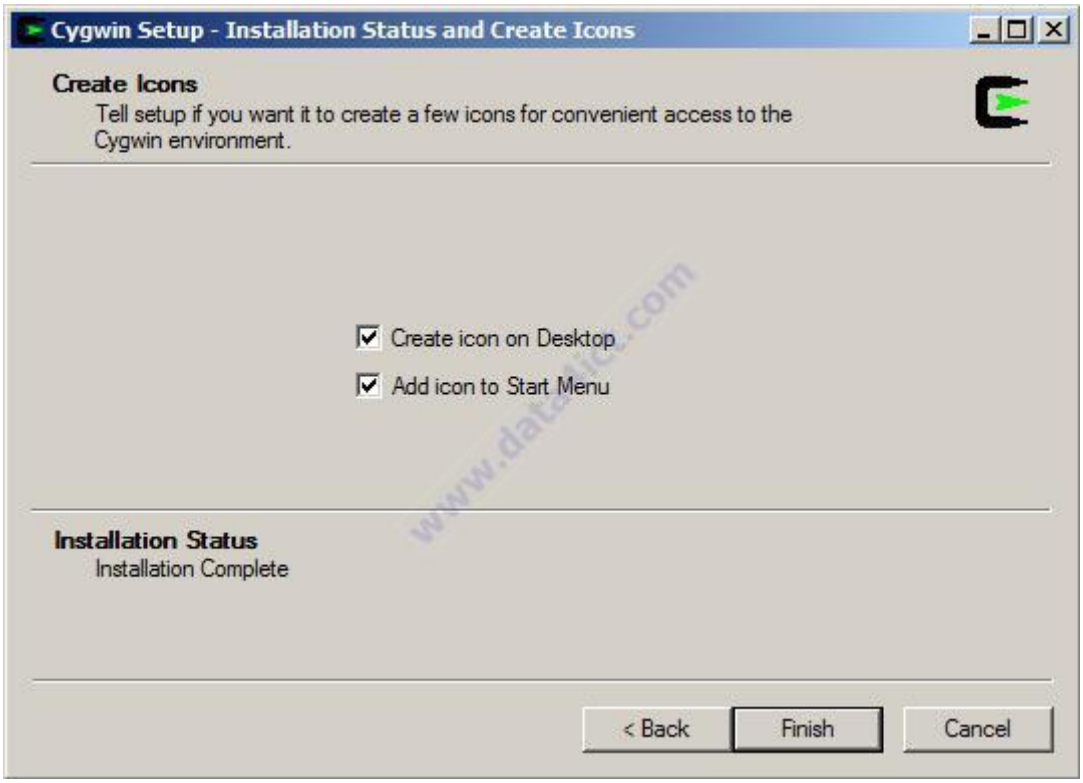


Рис. 6.34. Установка cygwin

Настройка модулей

Чтобы избежать ошибок при запуске программы, нужно настроить файл "modules.conf". Откройте "C:\cygroot\asterisk\etc\modules.conf" файл с помощью блокнота и добавьте следующие строки в конце файла:

noload = pbx_dundi.so

noload = chan_capi.so

noload = chan_fx.so

noload = chan_tapi.so

И удалите:

noload = app_queue.so

В итоге файл должен выглядеть так

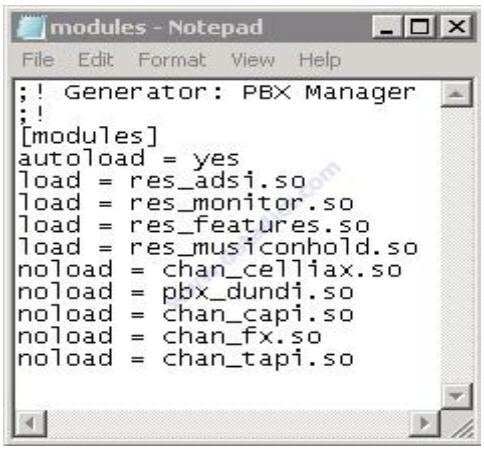


Рис. 6.35. Настройка файла "modules.conf

Теперь снова попробуйте запустить AsteriskW32 GUI , ошибок возникнуть не должно.

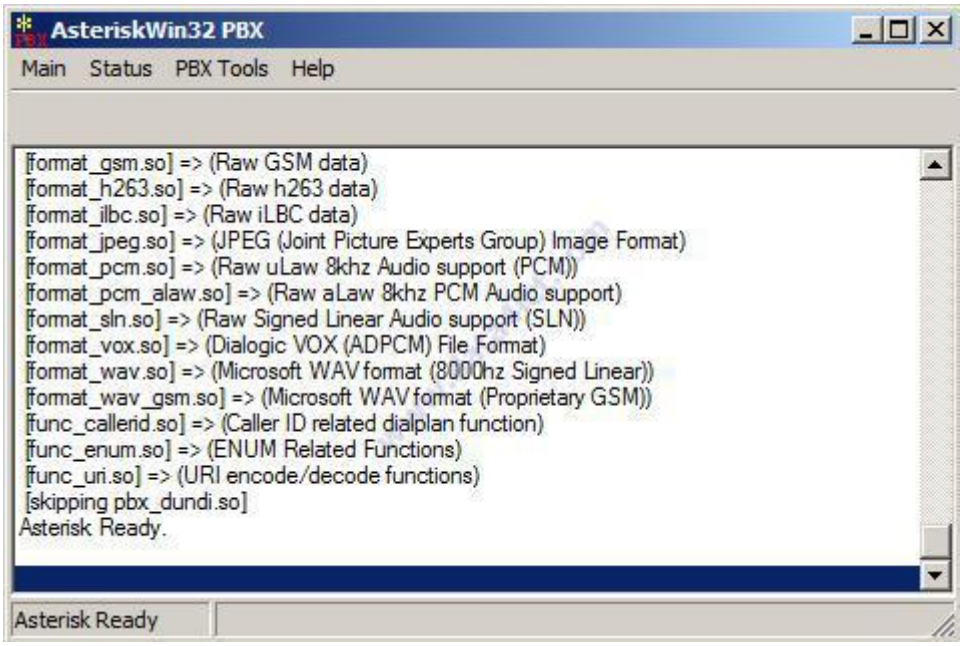


Рис. 6.36. Запуск AsteriskWin32

Настройка Windows Firewall

Откройте Windows Firefall

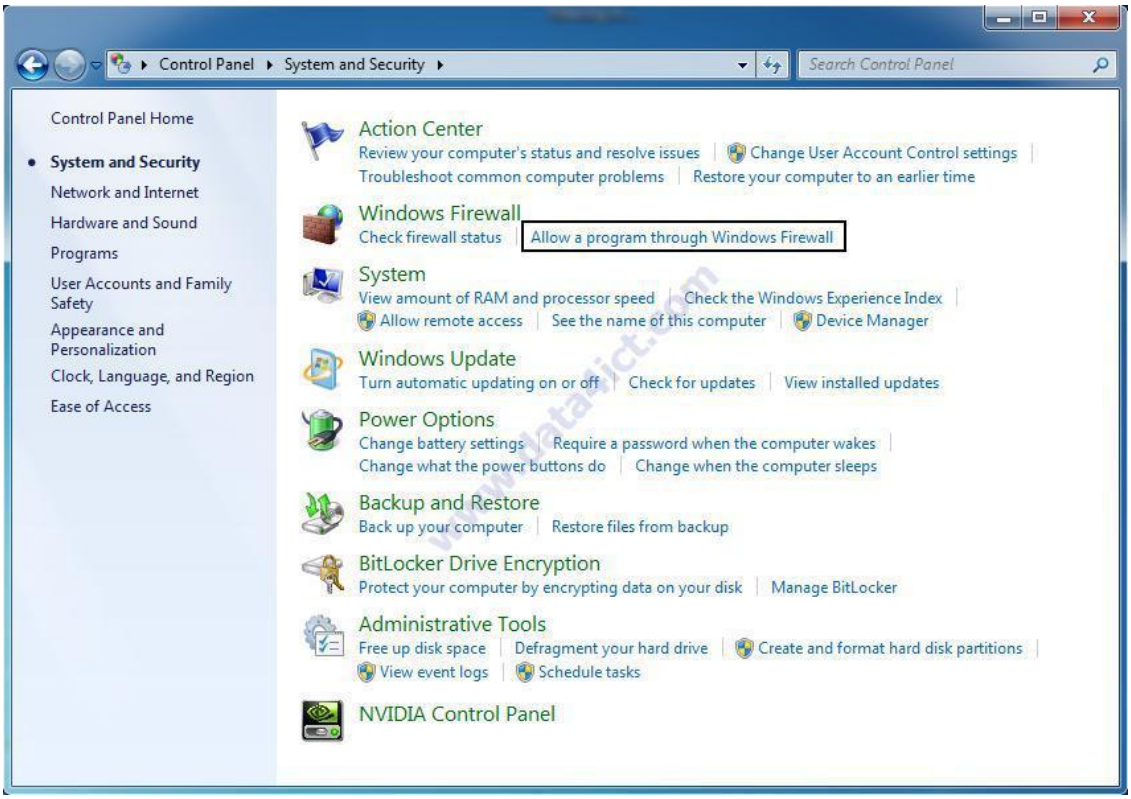


Рис. 6.37. Запуск Windows Firewall

Затем кликните настройки

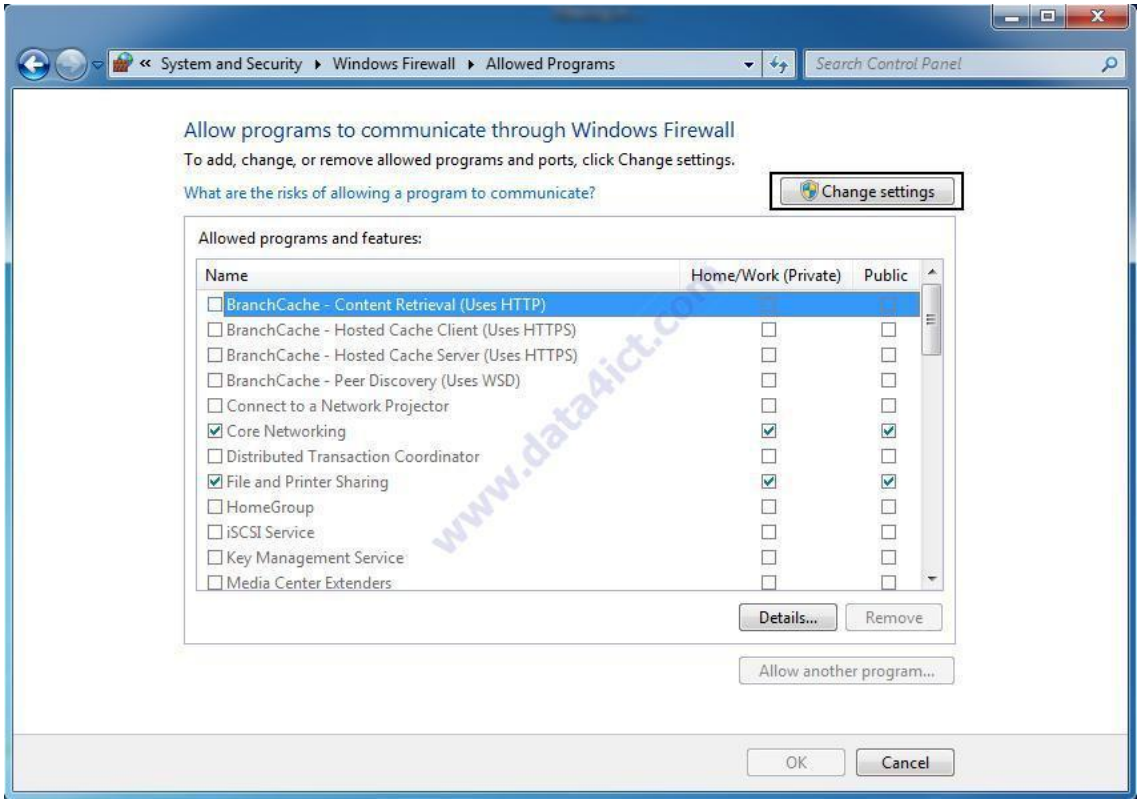


Рис. 6.38. Запуск Windows Firewall

Выберите добавить другую программу

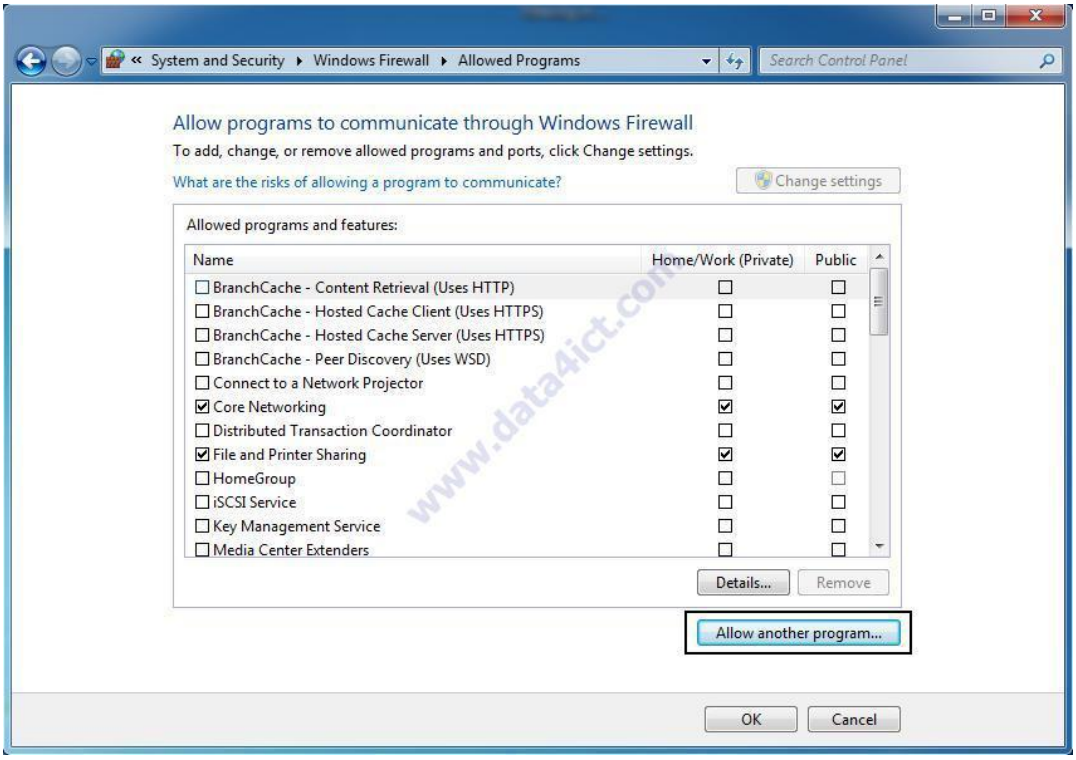


Рис. 6.39. Запуск Windows Firewall

Найдите в списке AsteriskWin32 GUI и нажмите добавить, затем закройте все окна с Windows Firefall

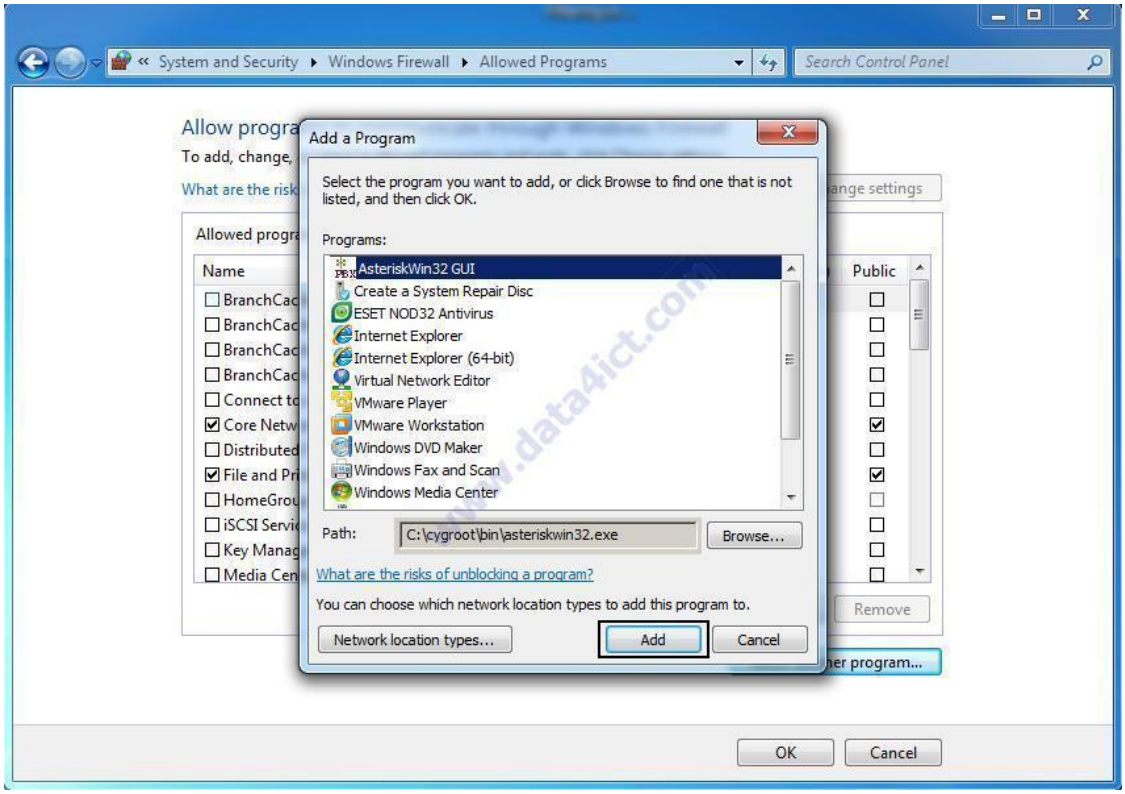


Рис. 6.40. Запуск Windows Firewall

Регистрация в AsteriskWin32

Asterisk имеет различные типы сообщений, которые могут быть зарегистрированы. К ним относятся:

debug

notice

warning

error

verbose

dtmf

logger.conf

Asterisk предоставляет ряд способов для регистрации . Файл logger.conf (Местонахождение: C:\cygroot\asterisk\etc\logger.conf) содержит элементы конфигурации для регистрирования.

;

; Logging Configuration

;

[general]

;

[logfiles]

debug => debug

messages => warning,error

console => notice,warning,error,debug,verbose,dtmf,fax

Первая строка говорит Asterisk, что войти log debug (правая сторона =>) в файл с именем отладки (на левом фланге из =>), расположенный в C:\cygroot\asterisk\log\.

Вторая строка сообщает Asterisk, что возможно зарегистрировать предупреждения и сообщения об ошибках в файл с именем сообщения, расположенные в C:\cygroot\asterisk\log\.

Третья строка говорит Asterisk отправлять все сообщения в CLI консоли.

asterisk.conf

Каталог журнала может быть изменен путем изменения линия astlogdir => asterisk/log to point, чтобы указать на нужный каталог в файле asterisk.conf (C:\cygroot\asterisk\etc\asterisk.conf).

Существуют различные уровни verbosity и debugging. Используйте установить многословным или установить отладки с последующим числовым значением их изменения.

Полезные значения от 0 (disabled) до 10 (maximum) за verbosity и отладки уровнях.

Выставите в окне PBX Manager set verbose 10

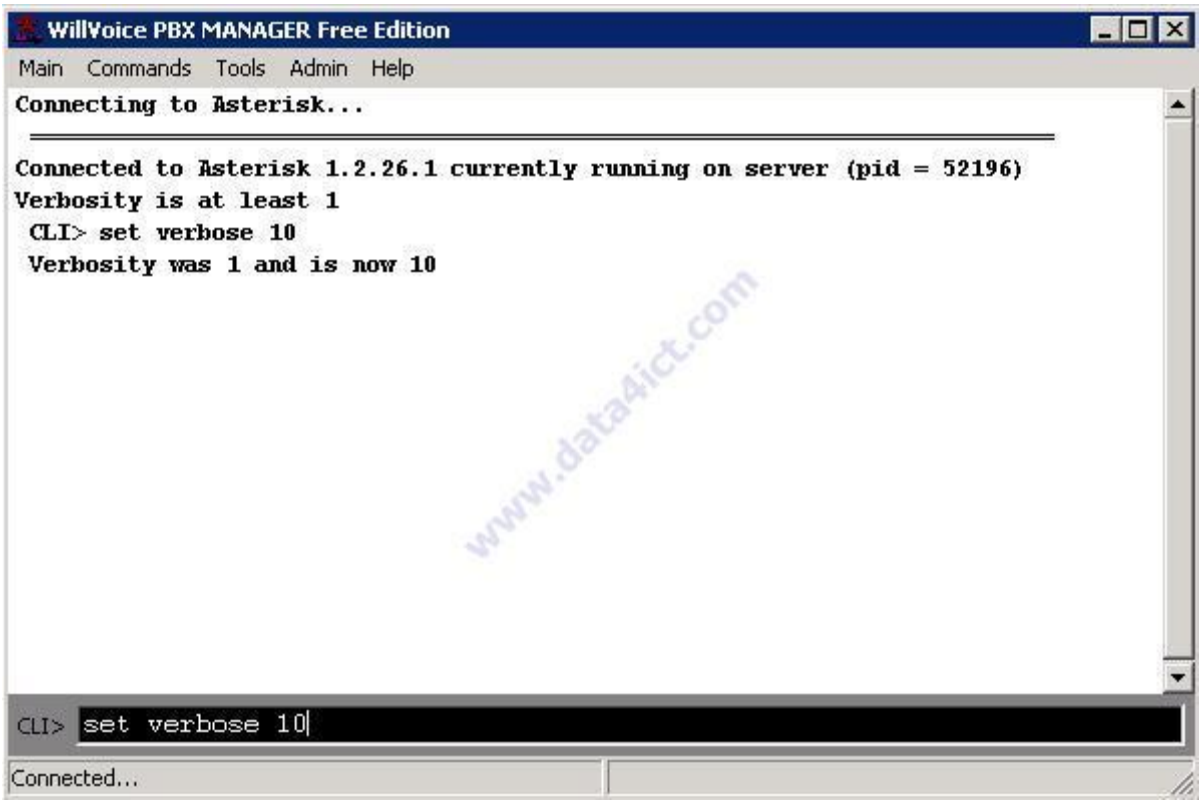


Рис. 6.41. Настройка PBX Manager

Затем выставите set debug 10

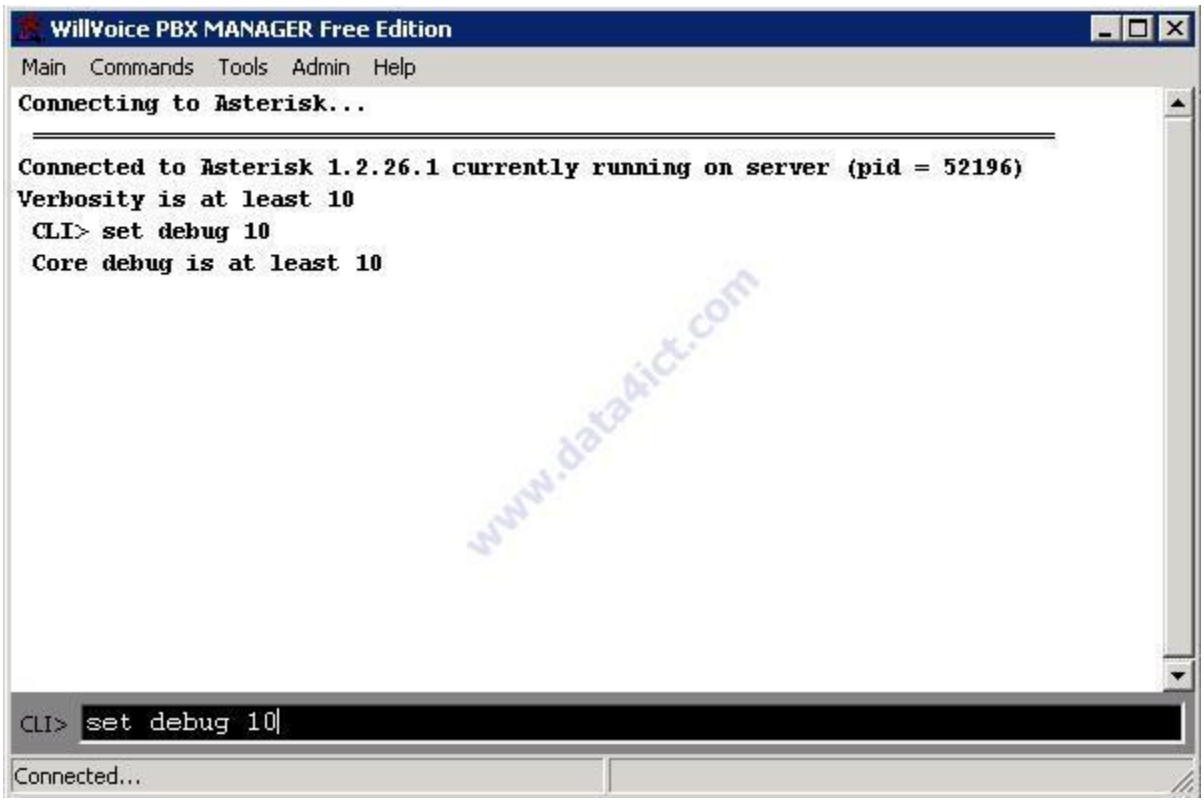


Рис. 6.42. Настройка PBX Manager

Так же возможно активировать другие типы отладки системы: (see asterisk CLI command)

debug channel / no debug channel

agi debug / agi no debug

iax2 debug / iax2 no debug

sip debug / sip no debug

Воспроизведение основных звонков

sip.conf

Измените название файла sip.conf file (Location: C:\cygroot\asterisk\etc\sip.conf) на sip_old.conf. Затем создайте новый файл sip.conf и вставьте следующее:

[general]

context = asterisk ; Default context for incoming calls

allowguest = no ; Allow or reject guest calls (default is yes, this can also be set to 'osp'

realm=data4ict.com ; Realm for digest authentication

bindport = 5060 ; UDP Port to bind to (SIP standard port is 5060)

bindaddr = 0.0.0.0 ; IP address to bind to (0.0.0.0 binds to all)

srvlookup = yes ; Enable DNS SRV lookups on outbound calls

disallow = all ; First disallow all codecs

allow = ulaw ; Allow codecs in order of preference

allow = alaw

allow = gsm

dtmfmode = rfc2833 ; Set default dtmfmode for sending DTMF.

canreinvite=no

nat=yes

[authentication]

[1001]

type=friend

context=asterisk

username=1001

secret=1001

host=dynamic

callerid="Phone1"

[1002]

type=friend

context=asterisk

username=1002

secret=1002

host=dynamic

callerid="Phone2"

extensions.conf

The second file to configure is the extensions.conf file (Location: C:\cygroot\asterisk\etc\extensions.conf). Rename it to extensions_old.conf and create a new extensions.conf empty file. Insert the following lines into the file:

Сконфигурируйте файл extensions.conf file (Location: C:\cygroot\asterisk\etc\extensions.conf). Переименуйте его в extensions_old.conf и создайте новый файл extensions.conf, включающий себя :

[general]

```
;
; If static is set to no, or omitted, then the pbx_config will rewrite
; this file when extensions are modified.  Remember that all comments
; made in the file will be lost when that happens.
static=yes
;
; if static=yes and writeprotect=no, you can save dialplan by
; CLI command 'save dialplan' too
;
writeprotect=yes
;
; If autofallthrough is set, then if an extension runs out of
; things to do, it will terminate the call with BUSY, CONGESTION
; or HANGUP depending on Asterisk's best guess (strongly recommended).
;
autofallthrough=yes
;
; If clearglobalvars is set, global variables will be cleared
; and reparsed on an extensions reload, or Asterisk reload.
;
clearglobalvars=no
;
; If priorityjumping is set to 'yes', then applications that support
; 'jumping' to a different priority based on the result of their operations
; will do so (this is backwards compatible behavior with pre-1.2 releases
; of Asterisk). Individual applications can also be requested to do this
; by passing a 'j' option in their arguments.
```

```
;
priorityjumping=yes
;
;[globals]
;
[internal]
exten => 1001,1,Dial(SIP/1001,20,Tr)
exten => 1001,2,Hangup()
exten => 1002,1,Dial(SIP/1002,20,Tr)
exten => 1002,2,Hangup()
[asterisk]
include => internal
;
; Create an extension, 600, for evaluating echo latency.
;
exten => 600,1,Playback(demo-echotest)    ; Let them know what's going on
exten => 600,2,Echo            ; Do the echo test
exten => 600,3,Playback(demo-echodone)    ; Let them know it's over
```

Настройка ответных звонков

sip.conf

Чтобы включить эту функцию, аккаунт нуждается в номере sip оператора.

С этим аккаунтом вы получите имя пользователя, пароль и sip- адрес или IP- адрес поставщика шлюза sip.

Конфигурация для основных и обратных звонков почти тоже самое, за исключением параметра "type=friend" становится "type=peer". Добавьте следующие строки в sip.conf file (Location: C:\cygroot\asterisk\etc\sip.conf).

```
[DATA4ICT]      - Your provider name
type=peer
username=1008100945      - Your account username
fromuser=1008100945      - Your account username
secret=aZ4kbY3i      - Your account password
host=178.63.114.87      - Your provider gateway
```

В sip.conf file до [general] добавить регистрационное определение:

```
register => 1008100945:aZ4kbY3i@178.63.114.87
```

В итоге файл sip.conf должен содержать:

```
[general]
context = asterisk          ; Default context for incoming calls
allowguest = no                 ; Allow or reject guest calls (default is yes, this can also be set to 'osp'
realm=data4ict.com              ; Realm for digest authentication
bindport = 5060             ; UDP Port to bind to (SIP standard port is 5060)
bindaddr = 0.0.0.0              ; IP address to bind to (0.0.0.0 binds to all)
srvlookup = yes             ; Enable DNS SRV lookups on outbound calls
videosupport = yes          ; Enable video
disallow = all                  ; First disallow all codecs
allow = ulaw                    ; Allow codecs in order of preference
allow = alaw
allow = gsm
allow = h263                    ; H.263 is our video codec
allow = h263p                   ; H.263p is the enhanced video codec
dtmfmode = rfc2833              ; Set default dtmfmode for sending DTMF.
canreinvite=no
nat=yes
register => 1008100945:aZ4kbY3i@178.63.114.87
 [authentication]
[1001]
type=friend
context=asterisk
username=1001
secret=1001
host=dynamic
callerid="Phone1"
[1002]
type=friend
context=asterisk
username=1002
secret=1002
host=dynamic
```

callerid="Phone2"

[DATA4ICT]

type=peer

username=1008100945

fromuser=1008100945

secret=aZ4kbY3i

host=178.63.114.87

extensions.conf

Во втором файле настройте extensions.conf (Местонахождение: C:\cygroot\asterisk\etc\extensions.conf). Вставьте следующую строку:

exten => _0.,1,Dial(SIP/DATA4ICT/${EXTEN})

В итоге файл должен содержать:

[general]

;

; If static is set to no, or omitted, then the pbx_config will rewrite

; this file when extensions are modified. Remember that all comments

; made in the file will be lost when that happens.

static=yes

;

; if static=yes and writeprotect=no, you can save dialplan by

; CLI command 'save dialplan' too

;

writeprotect=yes

;

; If autofallthrough is set, then if an extension runs out of

; things to do, it will terminate the call with BUSY, CONGESTION

; or HANGUP depending on Asterisk's best guess (strongly recommended).

;

autofallthrough=yes

;

; If clearglobalvars is set, global variables will be cleared

; and reparsed on an extensions reload, or Asterisk reload.

;

clearglobalvars=no

;

```
; If priorityjumping is set to 'yes', then applications that support
; 'jumping' to a different priority based on the result of their operations
; will do so (this is backwards compatible behavior with pre-1.2 releases
; of Asterisk). Individual applications can also be requested to do this
; by passing a 'j' option in their arguments.
;
priorityjumping=yes
;
;[globals]
;
[internal]
exten => 1001,1,Dial(SIP/1001,20,Tr)
exten => 1001,2,Hangup()
exten => 1002,1,Dial(SIP/1002,20,Tr)
exten => 1002,2,Hangup()
[asterisk]
include => internal
;
; Create an extension, 600, for evaluating echo latency.
;
exten => 600,1,Playback(demo-echotest); Let them know what's going on
exten => 600,2,Echo                     ; Do the echo test
exten => 600,3,Playback(demo-echodone)      ; Let them know it's over

exten => _0.,1,Dial(SIP/DATA4ICT/${EXTEN})
```

Установка ПО

ПО на первом компьютере (серверный)

Сейчас основная установка системы завершена. Скачайте софтфон X-Lite (бесплатный sip телефон) и установите его. Линк: http://www.counterpath.com/x-lite-download.html/.

Двойной клик по скачанному файлу"X-Lite_Win32_4.0_58832" и начнется установка. После запустите программу, кликните "Softphone", затем по "Account Settings"

Рис. 6.43. Настройка X-Lite

В поле User ID введите : 1001

- Domain: IP address of the asterisk server
- Password: 1001
- Display name: 1001
- Click "OK"

Как показано на рисунке 2.44

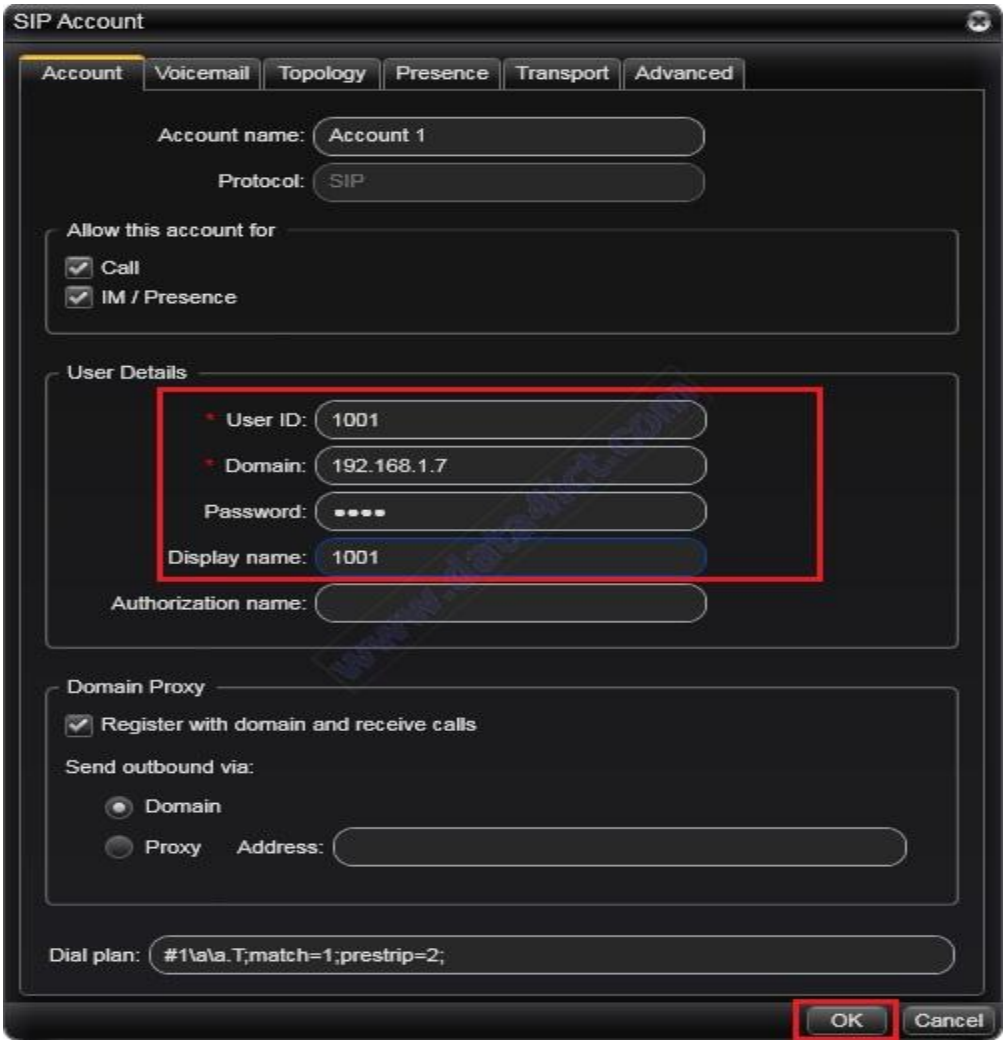


Рис. 6.44. Регистрация абонента

После регистрации , телефон готов производить звонки.

X-Lite (Второй компьютер)

Установите Xlite на втором компьютере по следующим конфигурациям:

User ID: 1002

Domain: IP address of the asterisk server

Password: 1002

Display name: 1002

Проверка

Откройте AsteriskWin32 PBX, откройте вкладку Status, затем CLI Console.

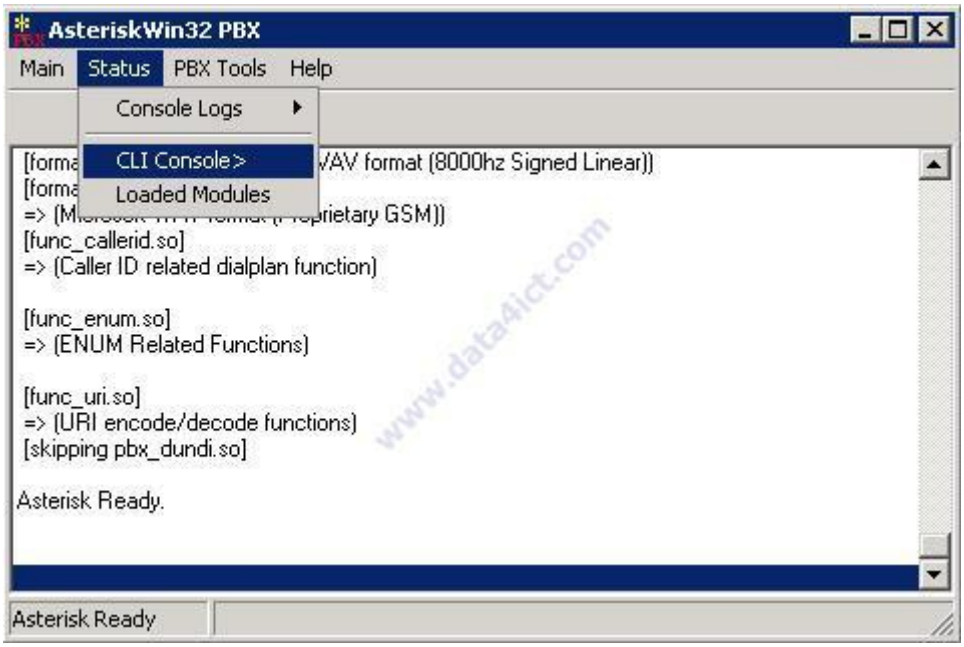


Рис. 6.45. Проверка правильности регистрации абонентов

В открытом окне CLI Console введите команду sip show peers, эта команда позволит просмотреть сведения о зарегистрированных абонентах в сети.

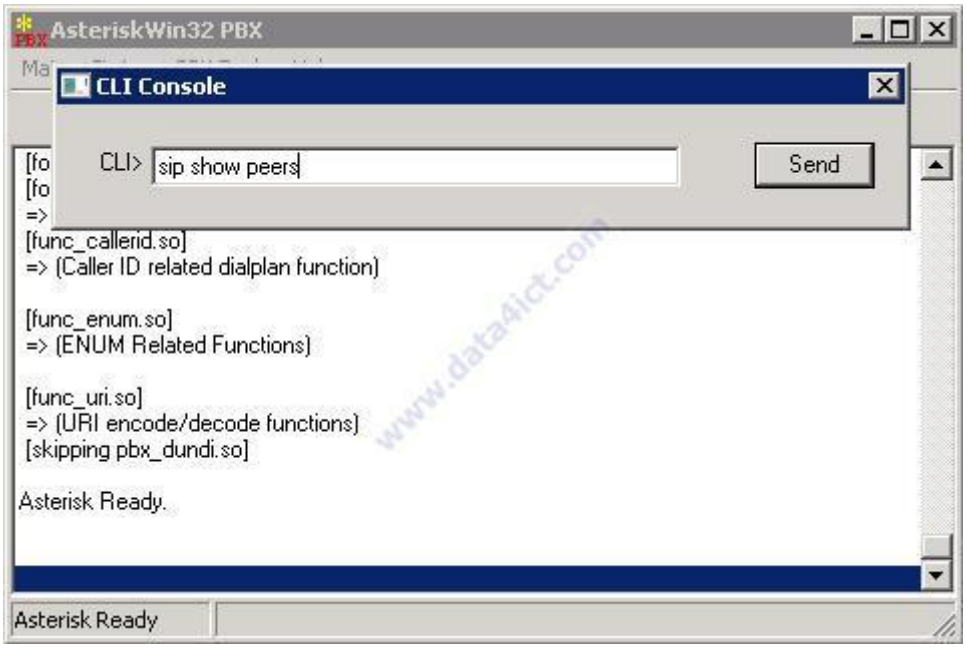


Рис. 6.46. CLI Console

Если все сделали по инструкции, то должно вывести информацию об абонентах: Имя,IP-адрес, Порт, Статус.

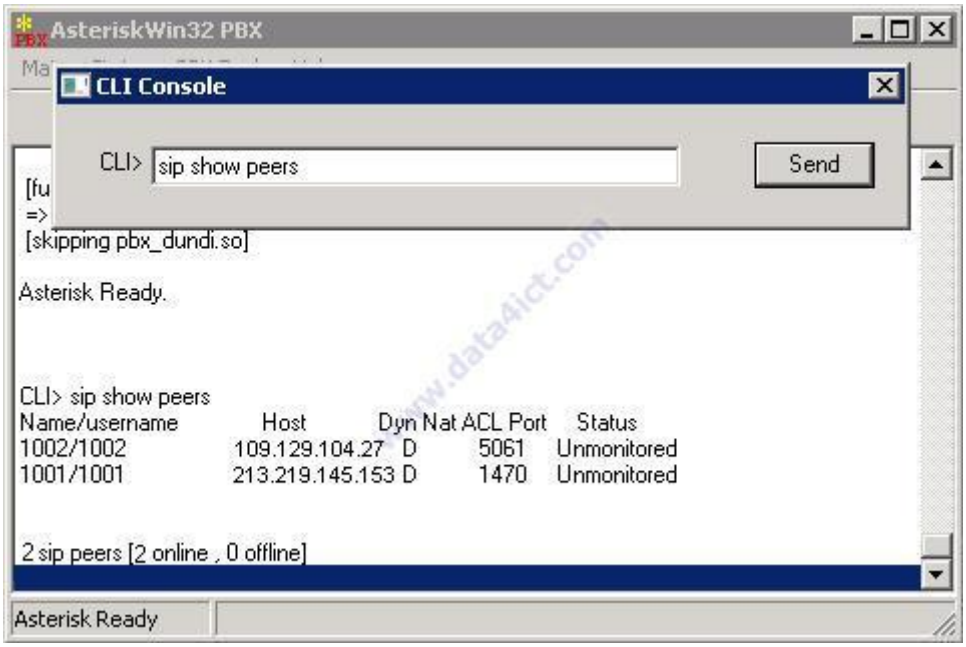


Рис. 6.47. Информация об абонентах

6.2. Проектирование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения VIPNET OFFICE

В связи с широким распространением персональных компьютеров не только как средств обработки информации, но и как оперативных средств коммуникации (электронная почта), возникают проблемы, связанные с обеспечением защиты информации от ее перехвата, преднамеренных или случайных искажений. Развитие информационных технологий сопровождается, к сожалению, ростом компьютерных преступлений, связанных с хищением конфиденциальной и другой информации, а также обусловленных этим обстоятельством материальных потерь. Первое компьютерное преступление, совершенное в городе Миннеаполисе в 1958 г., состояло в подделке банковских документов с помощью компьютера. По некоторым данным, утечка 20 % коммерческой информации в 60 % случаев приводит к банкротству фирмы. И это немудрено, поскольку по существующей статистике при ограблении банка потери (в среднем) составляют 19 тысяч долларов, а при компьютерном преступлении – 560 тысяч долларов.

Актуальность проблемы защиты информации подчеркивается тем обстоятельством, что персональный компьютер или автоматизированное рабочее место является частью систем обработки информации, систем коллективного пользования, вычислительных сетей.

Причины активизации компьютерных преступлений заключаются именно в том, что информационные технологии позволили реализовать идею академика В. М. Глушкова о безбумажных технологиях [1], создающих «…прочную основу для перестройки управления социально-экономическими процессами на основе безбумажной технологии в масштабах целой отрасли, крупного региона и даже целой страны». Однако обоснованное им еще в XX в. объединение вычислительных машин в крупные сети, впоследствии реализованное в виде всемирной сети Интернет, вызвало необходимость в предъявлении достаточно жестких требований к надежности и достоверности передаваемой информации, к предотвращению несанкционированного доступа к документам, передаваемым по сетям связи.

ViPNet OFFICE

ViPNet OFFICE — программное обеспечение для организации виртуальных частных защищенных сетей (VPN) типовых конфигураций (защищенных сетей ViPNet™). ViPNet OFFICE предназначен для использования в небольших локальных и распределенных IP-сетях и обеспечивает защищенную работу удаленных пользователей с любым типом подключения к сети Интернет.

ViPNet OFFICE — это программный комплекс, в состав которого входит три основных компонента:

ViPNet Manager (Менеджер) — рабочее место Администратора защищенной сети, предназначенное для развертывания и управления VPN-сетью. ViPNet Менеджер обладает интерфейсом, удобным и доступным даже для неподготовленных пользователей, что позволяет более простым и понятным образом задавать и изменять структуру защищенной VPN-сети.

ViPNet Coordinator (Координатор) — серверное программное обеспечение, которое выполняет функции межсетевого экрана, сервера IP-адресов, сервера защищенной почты.

ViPNet Client (Клиент) — программное обеспечение, которое устанавливается на рабочее место пользователя и выполняет функцию персонального сетевого экрана. В состав ViPNet Client входят такие программы как «Деловая почта», «Файловый обмен», «Обмен защищенными сообщениями» (чат), «Контроль приложений», а также поддерживаются механизмы ЭЦП — всё это делает рабочее место пользователя не только защищенным, но и многофункциональным.

При первоначальном развертывании ViPNet OFFICE обладает фиксированной конфигурацией. Существуют 4 фиксированные конфигурации:

ViPNet OFFICE 1–5 (1 — ViPNet Менеджер, 1 — ViPNet Координатор, 5 — ViPNet Клиент, 5 — туннельных лицензий);

ViPNet OFFICE 2–10 (1 — ViPNet Менеджер, 2 — ViPNet Координатор, 10 — ViPNet Клиент, 10 — туннельных лицензий);

ViPNet OFFICE 2–0 (1 — ViPNet Менеджер, 2 — ViPNet Координатор, 20 — туннельных лицензий);

ViPNet Office 3–0 (1 — ViPNet Менеджер, 3 — ViPNet Координатор, 30 — туннельных лицензий).

Основные отличия между ViPNet CUSTOM и ViPNet OFFICE:

Основное отличие программного комплекса ViPNet OFFICE от ViPNet CUSTOM состоит в том, что для развертывания, модификации и управления защищенной VPN-сетью в ViPNet OFFICE используется ViPNet Manager, а не ViPNet Administrator.

ViPNet Manager обладает интерфейсом, удобным и доступным даже для неподготовленных пользователей, что позволяет более простым и понятным образом задавать и изменять структуру защищенной VPN-сети.

При необходимости, ViPNet OFFICE позволяет расширять фиксированную конфигурацию (путем добавления лицензий на программные компоненты ViPNet Coordinator и ViPNet Client), изменять количество туннельных лицензий, в зависимости от необходимого количества данных компонент в защищенной сети.

ViPNet OFFICE позволяет осуществлять межсетевое взаимодействие между двумя VPN-сетями, построенными как на базе ViPNet OFFICE, так и на базе ViPNet CUSTOM. Благодаря этому возможно организовать VPN-сети любых произвольных конфигураций.

Основные преимущества:

Простое и понятное программное обеспечение для создания защищенной сети, для использования которого не требуется специальных познаний в области защиты информации, а также приобретения дополнительного оборудования и изменения структуры уже существующей сети.

Минимальные затраты на создание и обслуживание собственной VPN-сети.

Надежная защита сетевого трафика, не мешающая работе дополнительных приложений и прикладных задач.

Гибкий подход к построению VPN-сетей на базе уникальных технологий ViPNet позволяет создавать и связывать между собой разные сети ViPNet, обеспечивать более гибкий подход к созданию различных сетевых конфигураций, создавать территориально распределенные подсети, управляемые из центрального офиса.

Мастер развертывания сети позволяет пошагово создать структуру сети без дополнительных настроек на сетевых узлах.

Возможность ограничивать интерфейс пользователя на сетевом узле позволяет централизованно управлять политиками безопасности в защищенной сети.

Автоматизированная обработка и прием запросов на сертификаты ЭЦП.

Совместимость с решениями Linux, включая возможность централизованного обновления ПО на Linux-координаторах и ПАК.

С помощью ViPNet OFFICE Вы сможете:

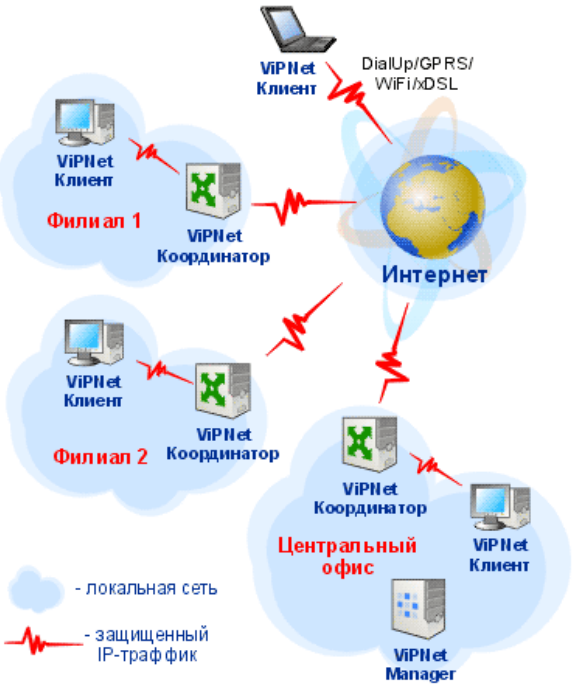
Обеспечить защищенный обмен данными, в том числе и защищенный документооборот между несколькими офисами или филиалами компании. При этом в каждом из филиалов может быть собственная VPN-сеть либо подсеть, управляемая из центрального офиса.

Организовать удаленный защищенный доступ сотрудников компании или руководства через Интернет к конфиденциальным ресурсам локальной сети компании и одновременно обеспечить защиту их мобильных компьютеров от возможных сетевых атак.

Обеспечить разграничение доступа внутри локальной сети, например, обеспечить доступ к серверу с конфиденциальной информацией определенной группе лиц, при этом остальные пользователи той же сети не будут даже подозревать о его существовании.

Обеспечить простое и удобное использование электронно-цифровой подписи как внутри VPN-сети, так и с помощью стандартных почтовых офисных приложений (Microsoft Outlook, Outlook Express).

Типовая схема защищенной сети на базе решения ViPNet OFFICE:



Комментарии к схеме:

ПО ViPNet Manager устанавливается в Центральном офисе компании.

ПО ViPNet Coordinator устанавливается в Центральном офисе и Филиалах компании, на входе в локальную сеть, на серверы-маршрутизаторы, и выполняет роль межсетевого экрана и криптошлюза для организации защищенных туннелей между удаленными локальными сетями.

ПО ViPNet Client может быть установлено как внутри локальных сетей (на рабочих станциях сотрудников), так и на мобильные компьютеры для организации защищенного удаленного доступа к ресурсам локальных сетей. ViPNet Client в этом случае выполняет роль персонального сетевого экрана и шифратора IP-трафика.

Одновременно с работой в защищенной сети ViPNet Coordinator и ViPNet Client могут выполнять фильтрацию обычного, незашифрованного IP-трафика, что позволяет обеспечить необходимую работу серверов и рабочих станций с открытыми ресурсами Интернета (веб-страницами) или локальных сетей (сетевыми принтерами, незащищенными рабочие станции и серверами).

Испытание системы защищенного межсетевого взаимодействия

В качестве объекта испытания будет выступать виртуальная сеть, состоящая из четырех виртуальных машин (далее ВМ), развернутая в среде VMwareWorkstation. На трех ВМ выполняется установка ПО ViPNetOFFICE, обеспечивая, таким образом, защищенное межсетевое взаимодействие в данном сегменте сети. Четвертая ВМ служит интересам предполагаемого злоумышленника и предназначена для захвата циркулирующего в сети трафика с помощью программы-сниффера Wireshark .

Данный макет моделирует межсетевое взаимодействие между компьютерами головного отделения и филиала учреждения посредствам открытых ССОП. Так как ССОП находятся вне контролируемой зоны, возможен перехват ПДн злоумышленником и нарушение их конфиденциальности, целостности и доступности.

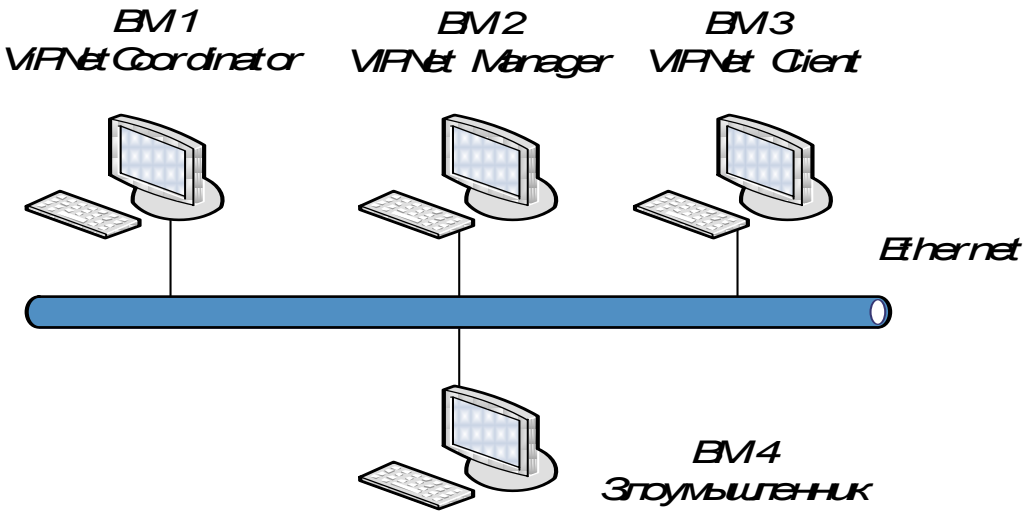


Рис. 6.47. Схема макета VIPNet

План испытания

Испытание состоит из нескольких этапов, характерной особенностью которых является исследование открытого и защищенного сетевого взаимодействия:

развораччивание виртуальной сети;

исследование открытого сетевого взаимодействия:

перехват и анализ текстового файла;

перехват и анализ ping-пакетов;

установка ПО ViPNetOFFICE;

исследование защищенного сетевого взаимодействия:

перехват и анализ текстового файла;

перехват и анализ ping-пакетов.

Ход испытания

Разворачивание виртуальной сети

После выполнения установки VMwareWorkstationв ней создаются четыре ВМ со следующими основными параметрами:

объем ОЗУ 512 Мбайт;

объем жесткого диска 10 Гбайт;

ОСWindowsXP.

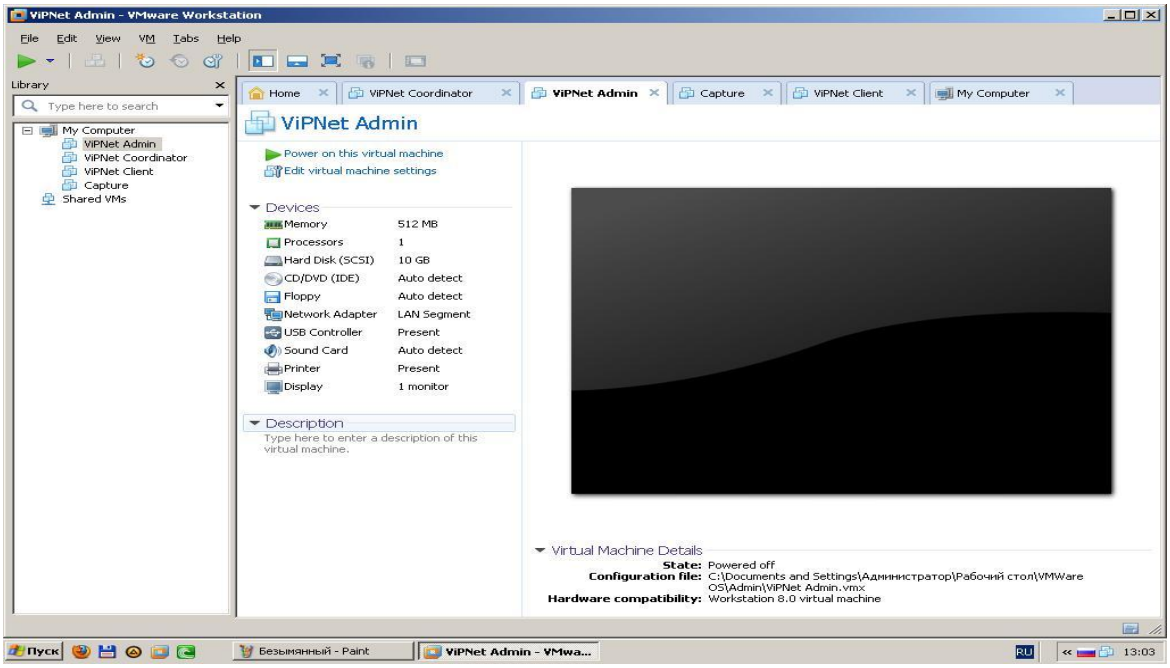


Рис. 6.48. ОбщийвидVMwareWorkstation

Виртуальные машины объединяются в виртуальную сеть с адресацией, представленной в таблице 6.4.

Таблица 6.4. Сетевая адресация виртуальных машин

	ВМ 1	ВМ 2	ВМ 3	ВМ 4
IPадрес	192.186.1.1	192.186.1.2	192.186.1.3	192.186.1.4
Маска подсети	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

На ВМ 4 устанавливается программа-сниффер Wireshark, с помощью которой захватывается и анализируется сетевой трафик. Процесс установки отображен на следующих рисунках.

Рис. 6.49. Мастер установки Wireshark

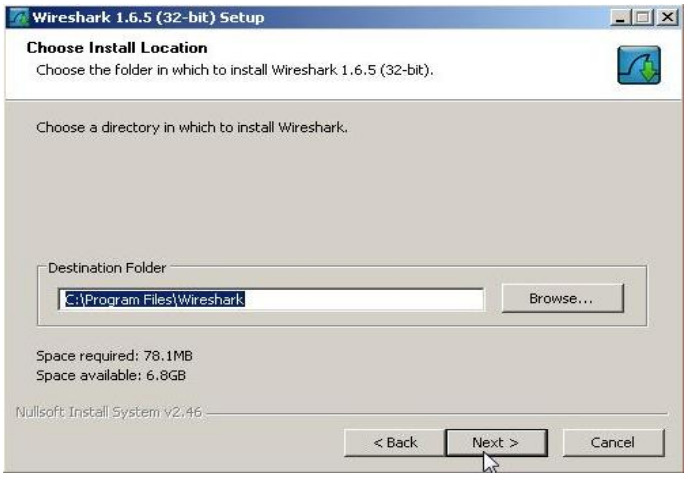


Рис. 6.50. Выбор директории установки

Рис. 6.51. Завершение установки

Исследование открытого сетевого взаимодействия

Для исследования открытого сетевого взаимодействия на ВМ 2 создается текстовый файл Test.txt, который передается на ВМ 3 по протоколу SMB (ServerMessageBlock).

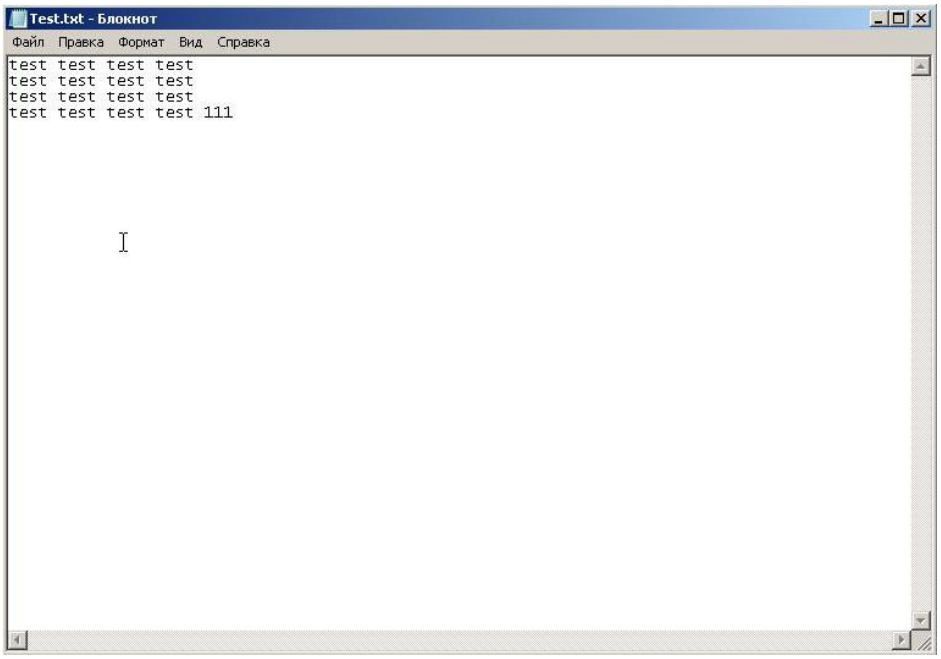


Рис. 6.52. Текстовый файл Test.txt

При передаче происходит захват пакетов на ВМ 4, что отображается в окне сниффера Wireshark. Протокол SMB принадлежит стеку TCP, поэтому при анализе отображается содержимое TCP-пакетов.

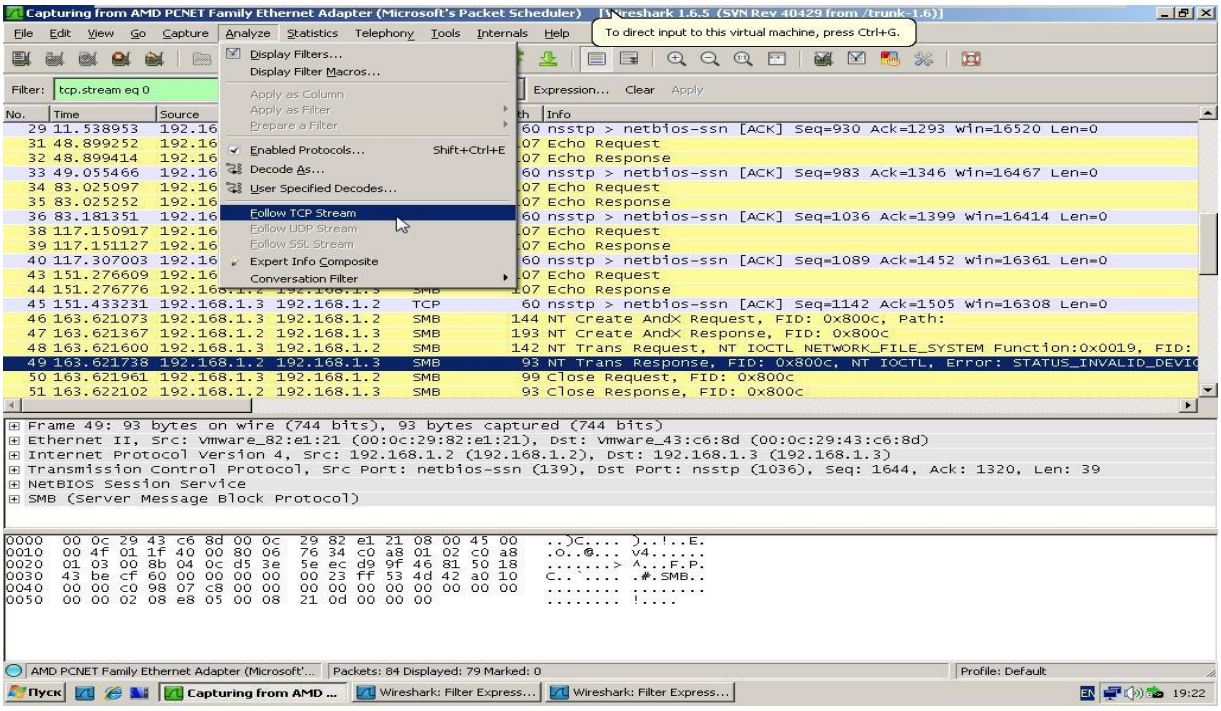


Рис. 6.53. Процесс отображения TCP-пакетов

На следующем рисунке видно, что среди содержимого пакетов отображается переданный текст файла Test.txt.

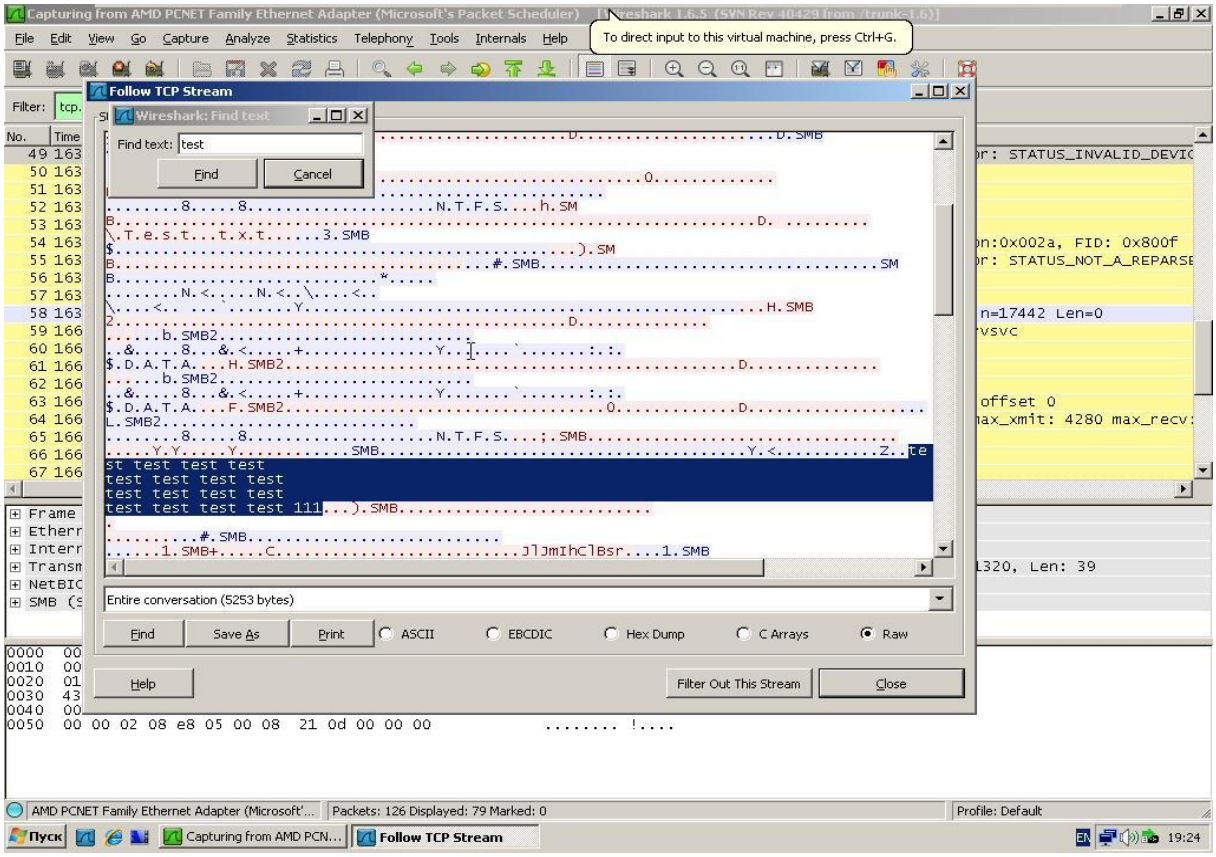


Рис. 6.54. Содержимое TCP-пакетов

Так же в программе Wireshark существует возможность работать с SMBтрафиком, то есть непосредственно перехватить передаваемый файл Test.txt. Этот процесс отображается на следующих рисунках.

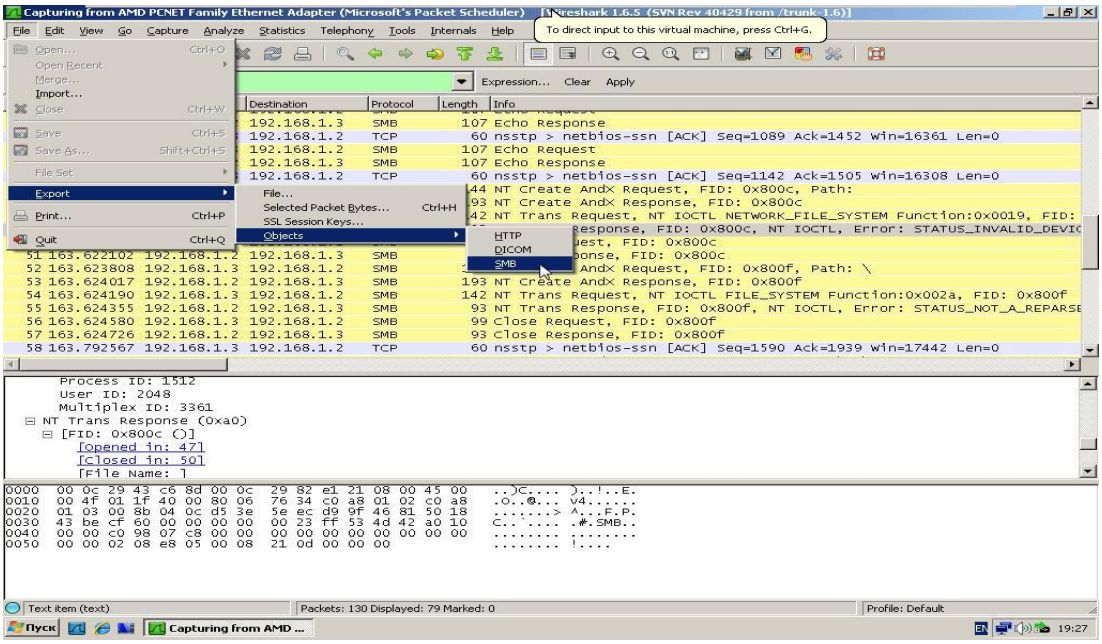


Рис. 6.55. Выбор SMB объекта для экспорта

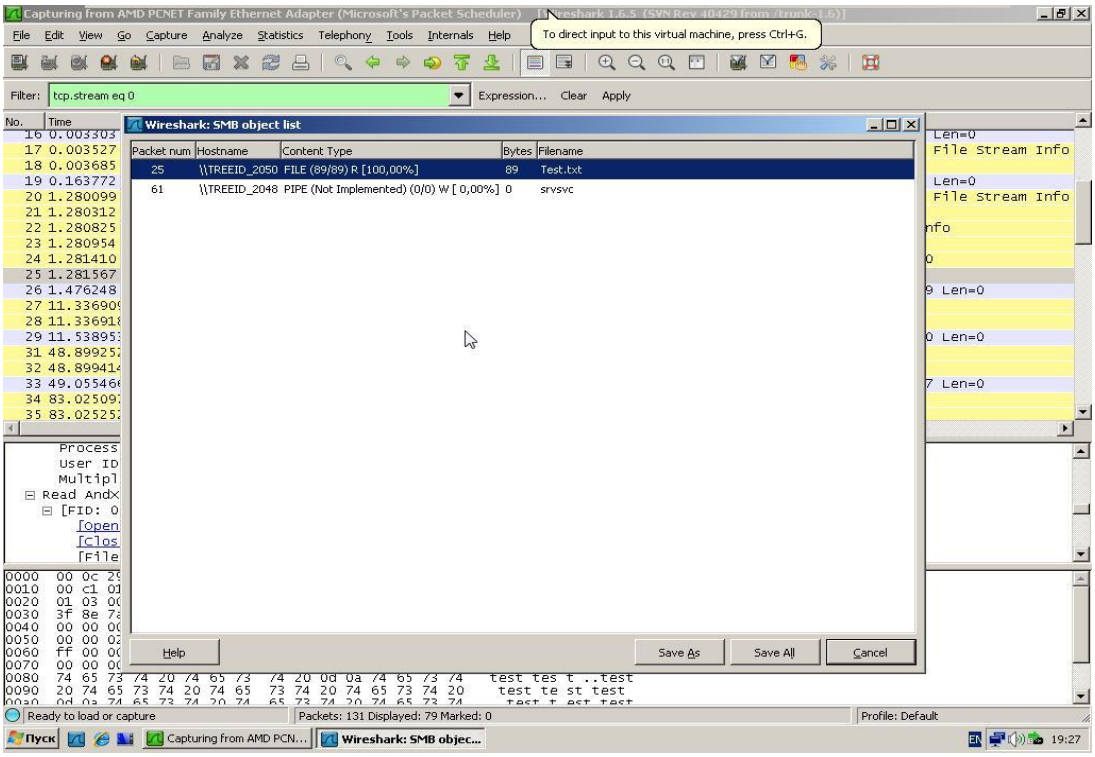


Рис. 6.56. Отображение захваченного SMB объекта

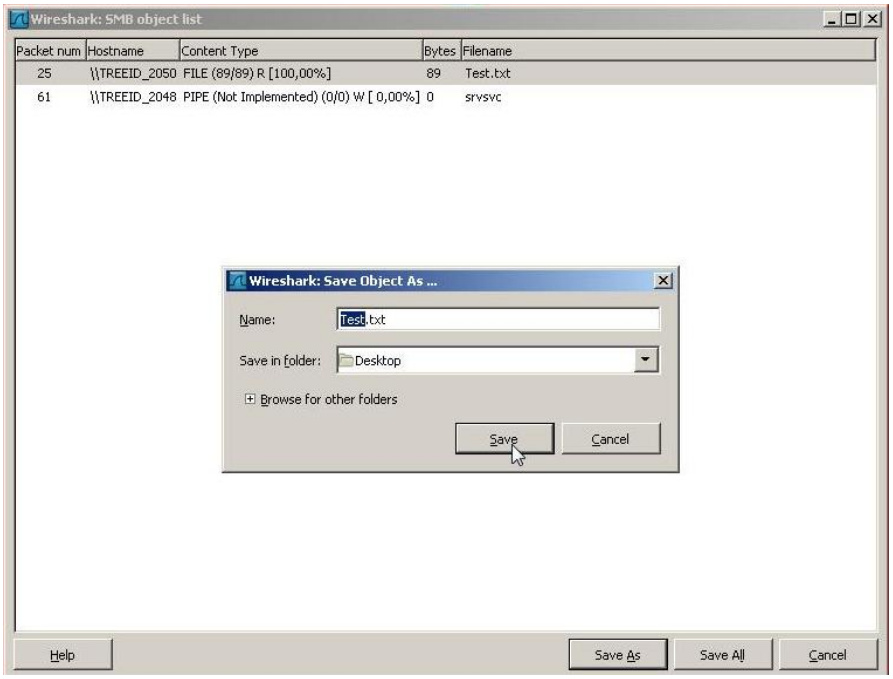


Рис. 6.57. Сохранение перехваченного объекта

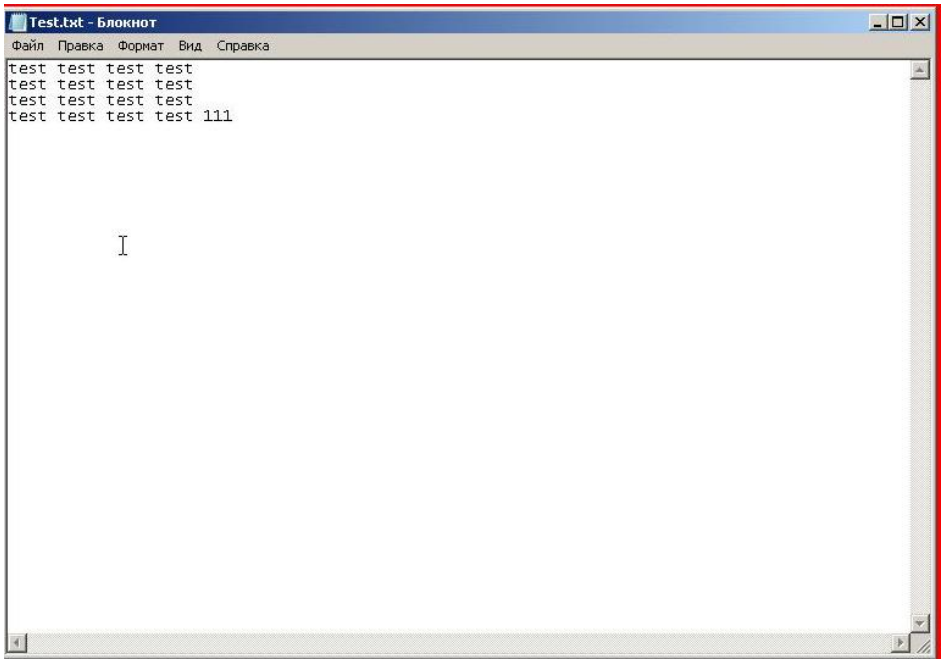


Рис. 6.58. Содержимое перехваченного объекта

Далее происходит запуск утилиты ping на ВМ 2 для проверки соединения с ВМ 3.

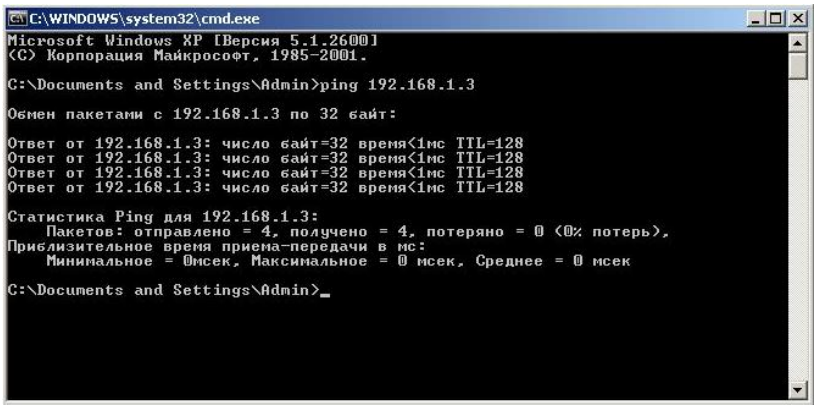


Рис. 6.59. Запуск утилиты ping

В результате в сети появляются ICMP-пакеты (Internet Control Message Protocol), которые захватываются снифферо м.

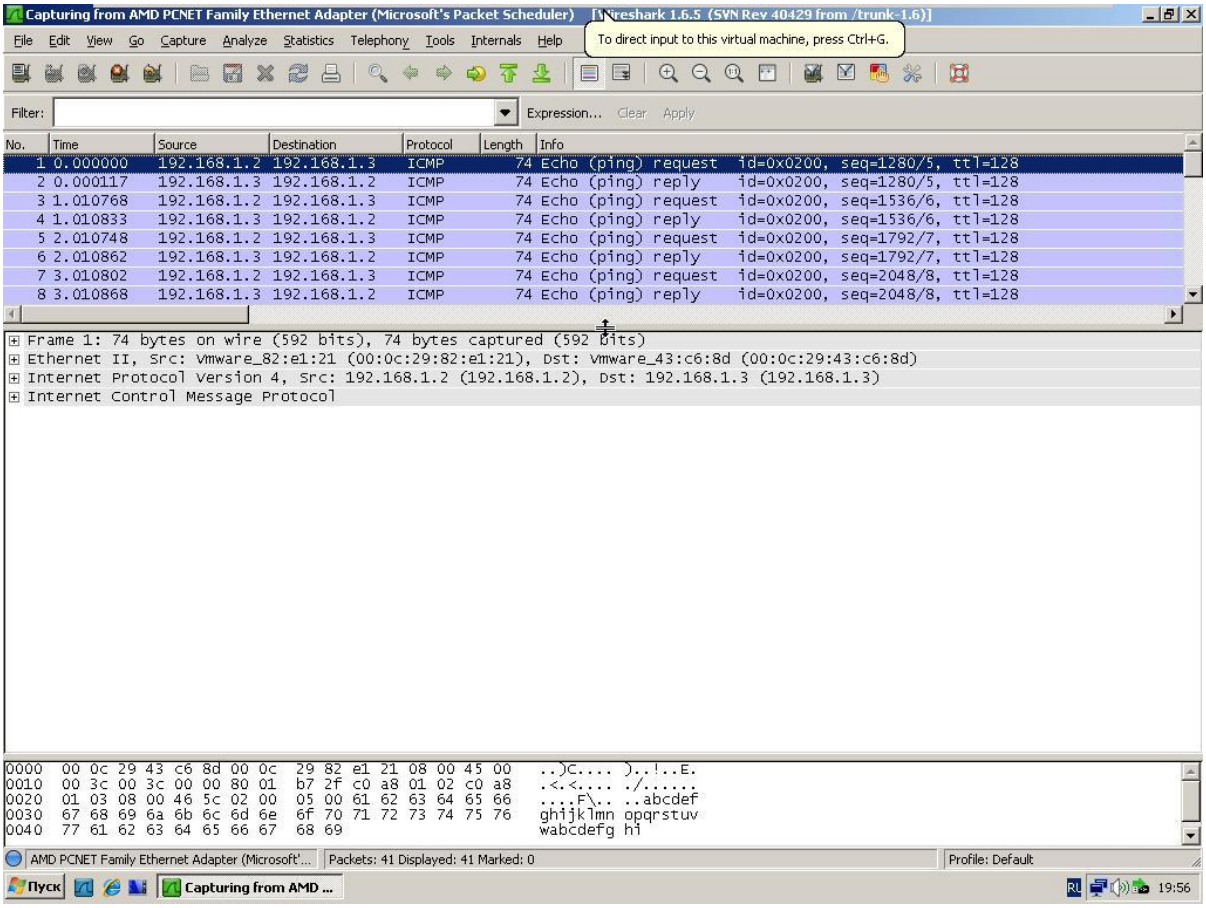


Рис. 6.60. Захваченные ICMP-пакеты

Таким образом, весь передаваемый трафик при передаче в открытом виде представляется неизменным, что подтверждается его анализом в сниффере.

Установка ПО ViPNet OFFICE

Для организации защищенного сетевого взаимодействия на ВМ устанавливается специализированное ПО ViPNet.

При этом в качестве менеджера (ViPNetManager) сети ViPNetвыступает ВМ 2, в качестве координатора (ViPNet Coordinator) сети – ВМ 1, и в качестве клиента (ViPNet Client) – ВМ 3. Процесс установки и конфигурирования ПО отображается на следующих рисунках.

Установка ПО начинается с установки ViPNet Manager и ViPNet Client на ВМ 2.

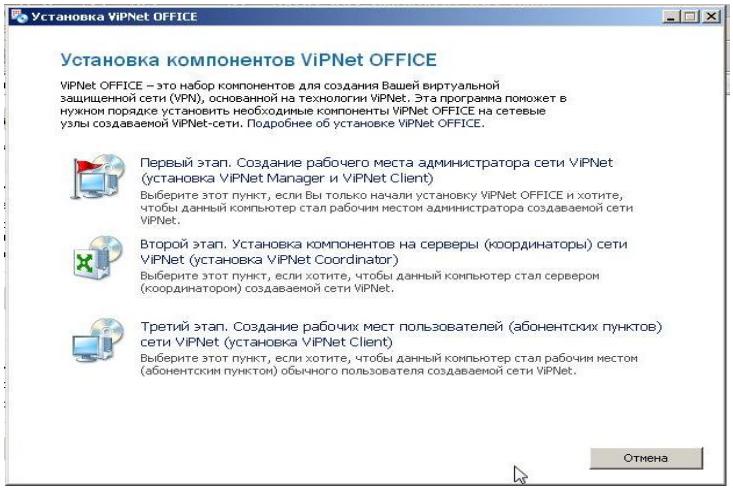


Рис. 6.61. Первый этап - создание рабочего места администратора сети ViPNet

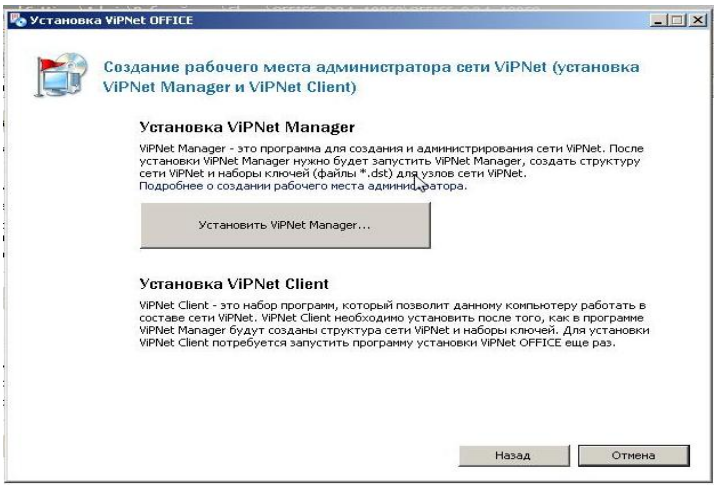


Рис. 6.62. Установка ViPNetManager

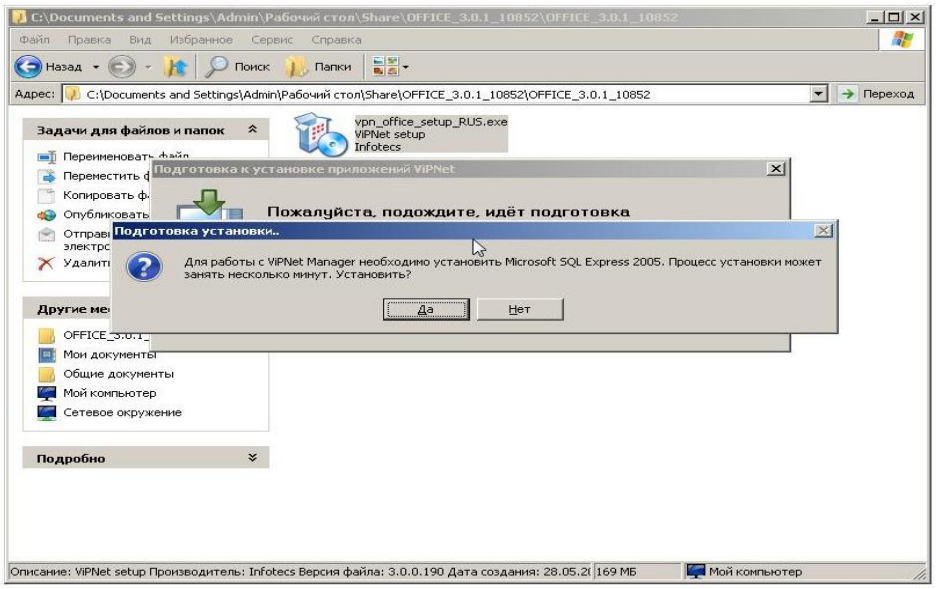


Рис. 6.63. Установка Microsoft SQL Express 2005

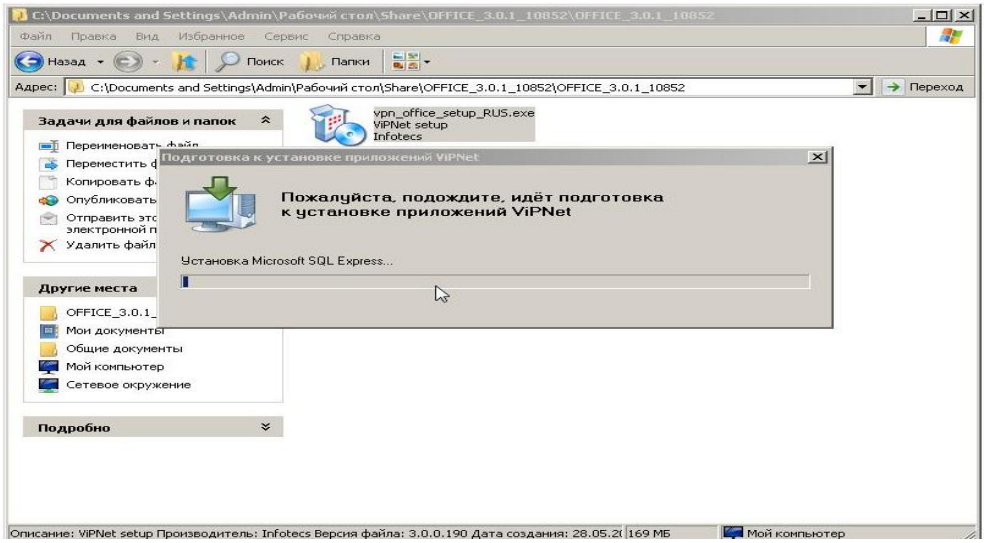


Рис. 6.64. Продолжение установки Microsoft SQL Express 2005

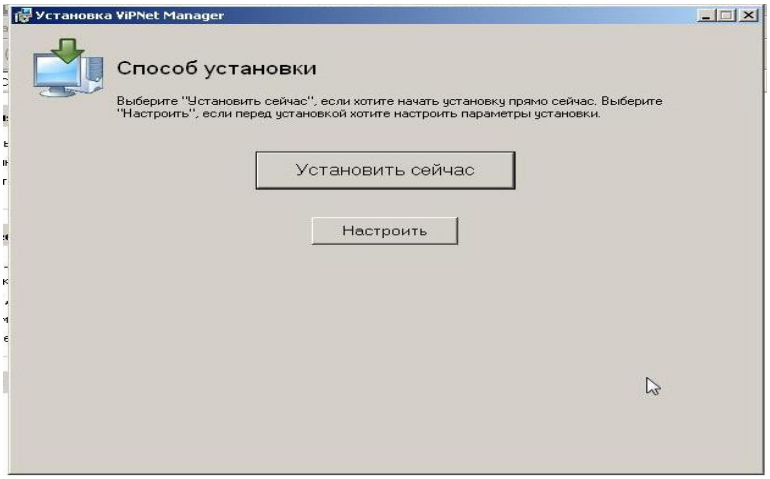


Рис. 6.65. Переход к установке ViPNet Manager

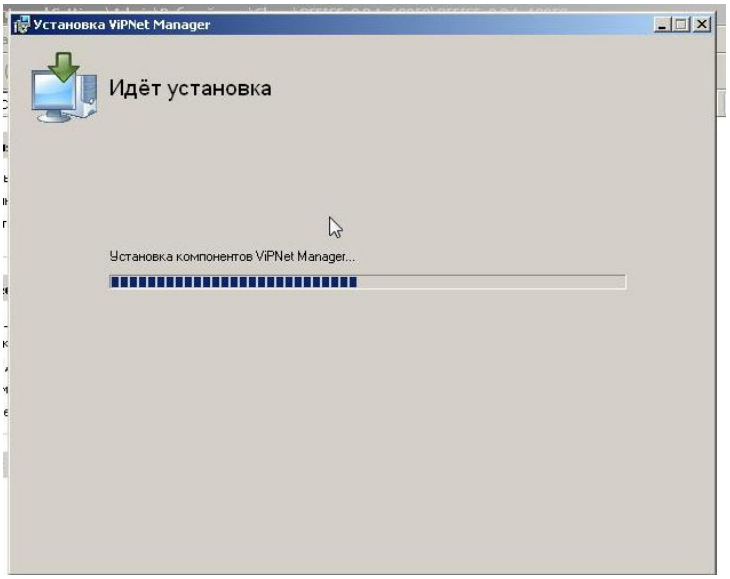


Рис. 6.66. Продолжение установки ViPNet Manager

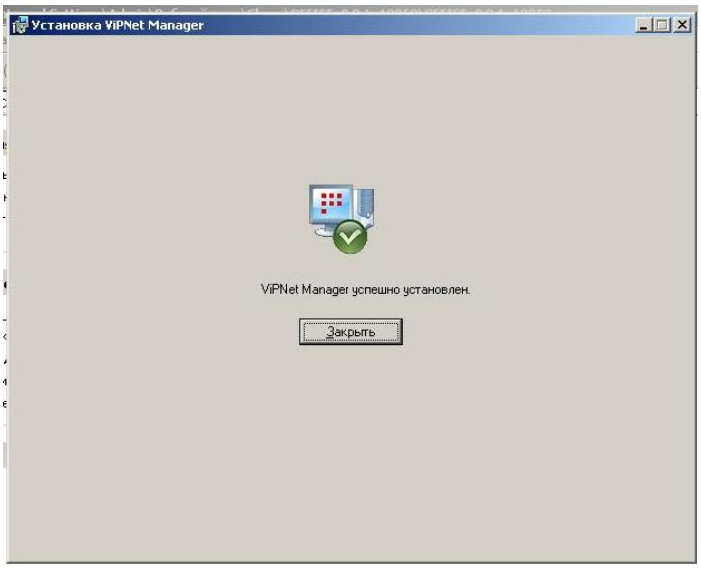


Рис. 6.67. Завершение установки ViPNetManager

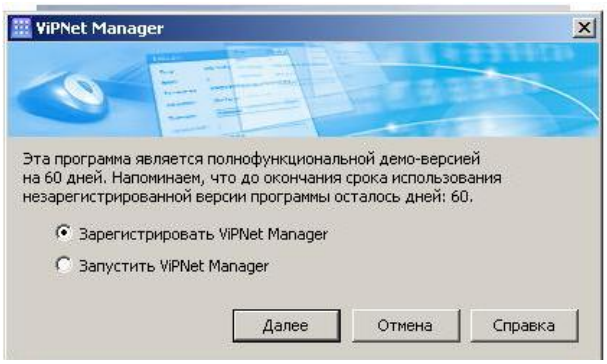


Рис. 6.68. Напоминание о том, что ПО является демо-версией

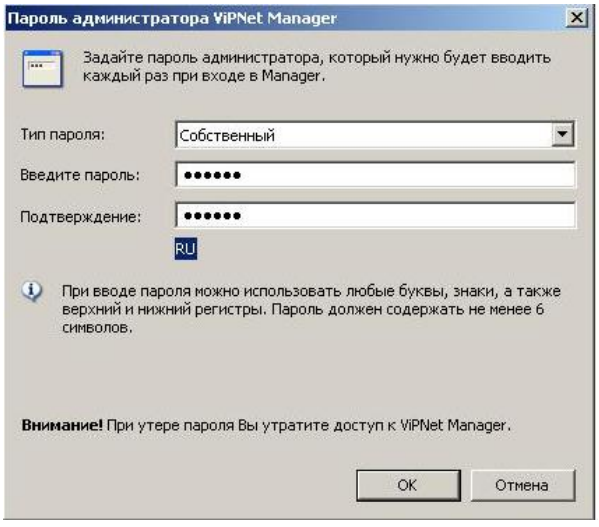


Рис. 6.69. Создание пароля администратора

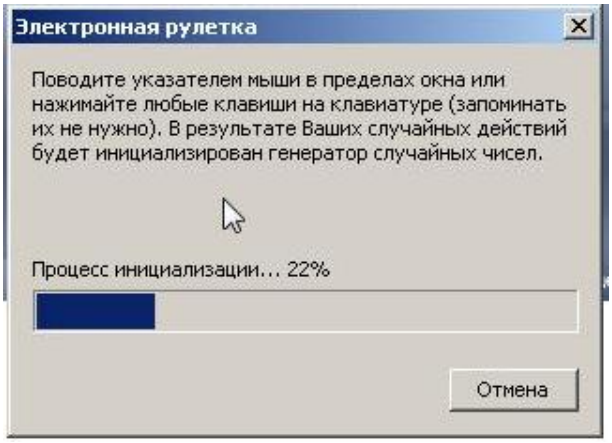


Рис. 6.70. Инициализация генератора случайных чисел

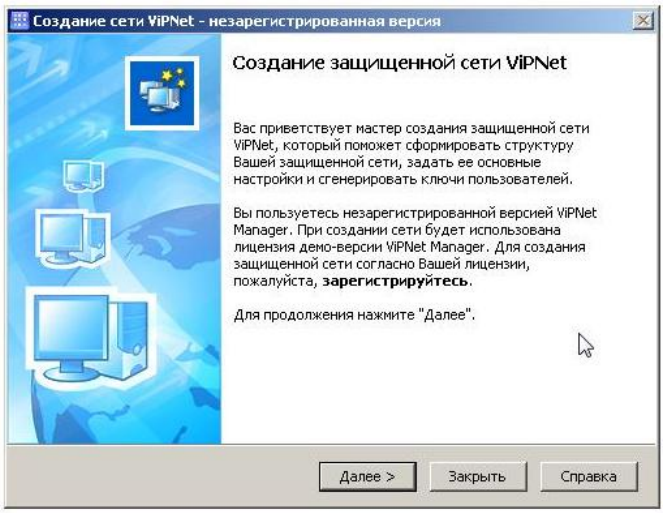


Рис. 6.71. Мастер защищенной сети Установка ViPNet

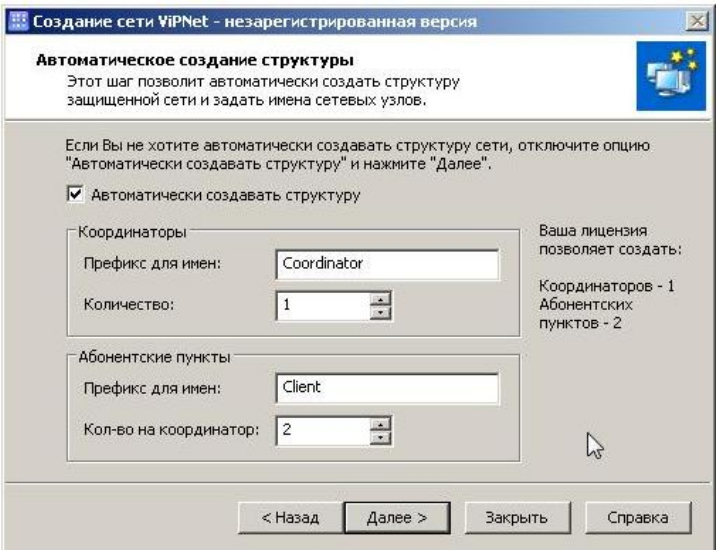


Рис. 6.72. Автоматическое создание структуры сети ViPNet

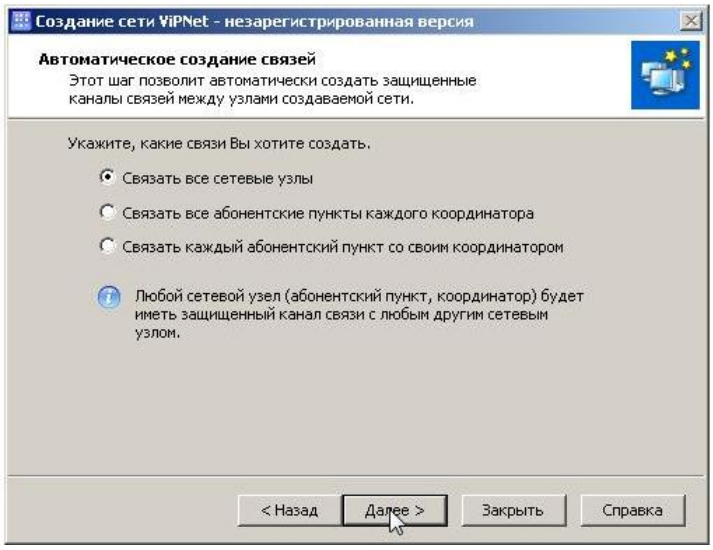


Рис. 6.73. Создание каналов связи между узлами сети ViPNet

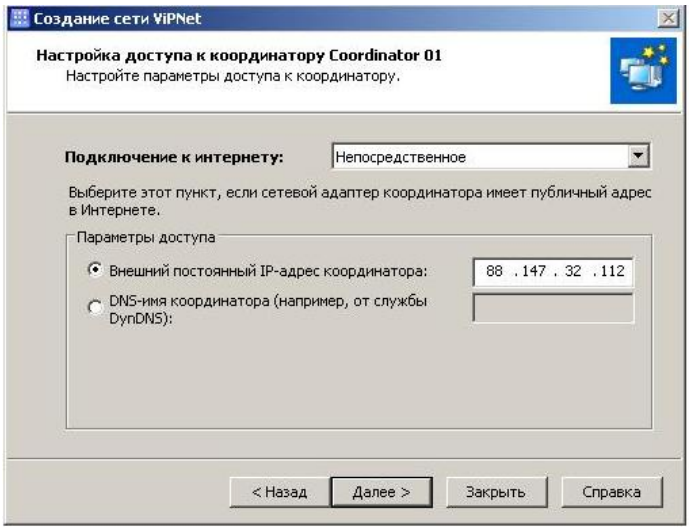


Рис. 6.74. Настройка доступа к координатору

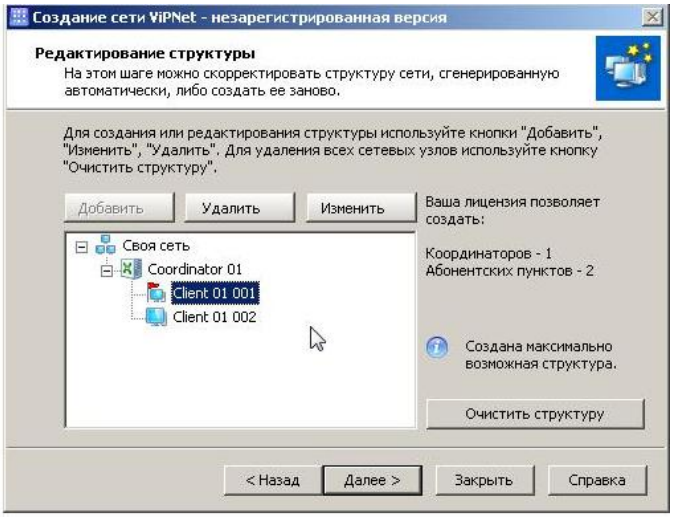


Рис. 6.75. Редактирование структуры сети ViPNet

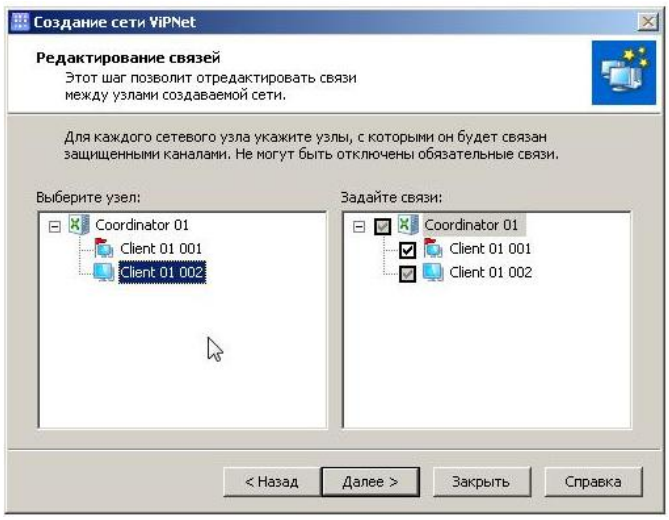


Рис. 6.76. Редактирование связей между узлами сети ViPNet

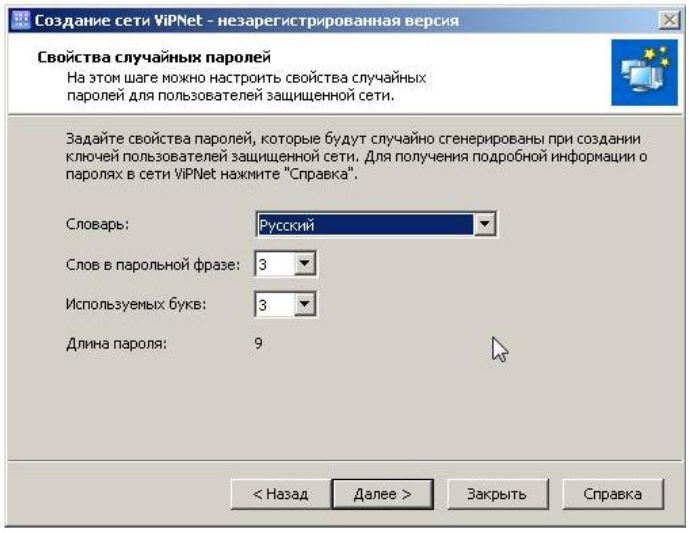


Рис. 6.77. Настройка паролей пользователей сети ViPNet

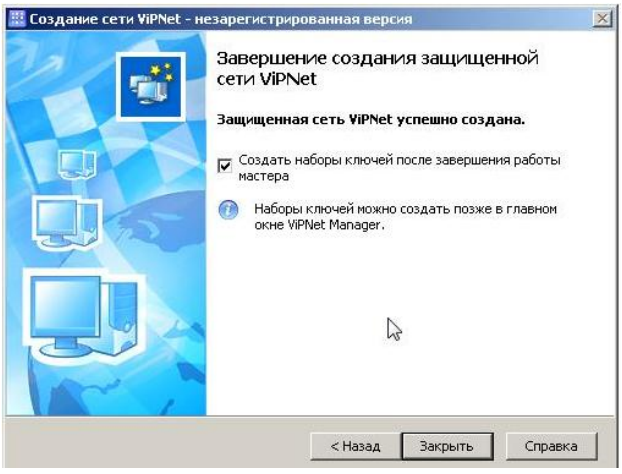


Рис. 6.78. Завершение работы мастера создания защищенной сети Установка ViPNet

Рис. 6.79. Запрос на сертификат сети ViPNet

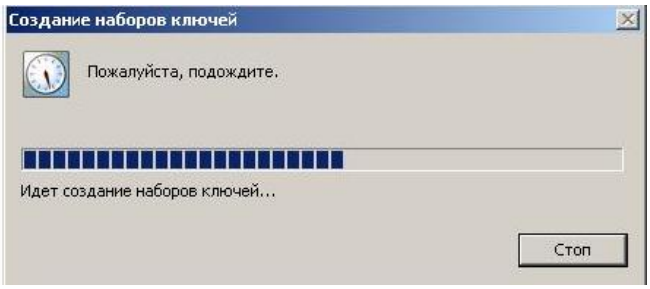


Рис. 6.80. Создание наборов ключей

Следующий шаг установка ПО ViPNet Client на рабочее место администратора (ВМ 2).

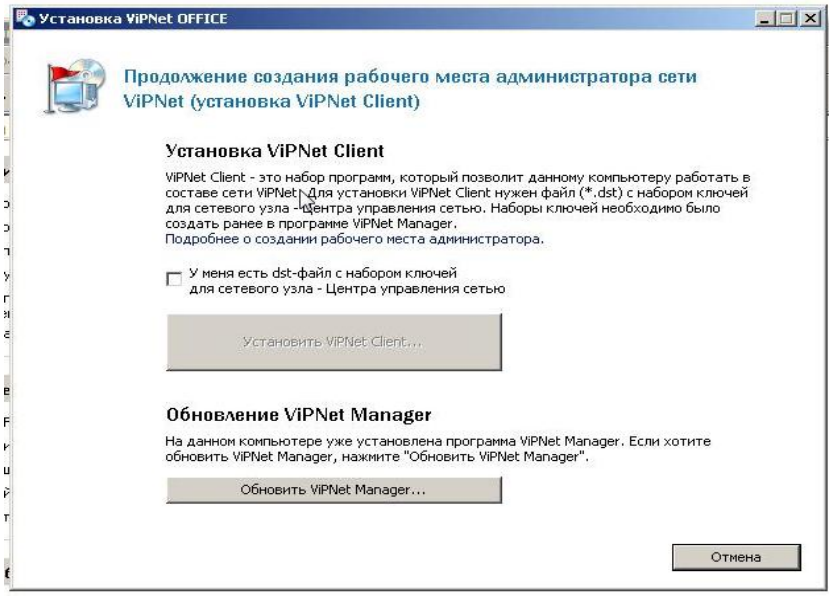


Рис. 6.81. Установка ViPNet Client

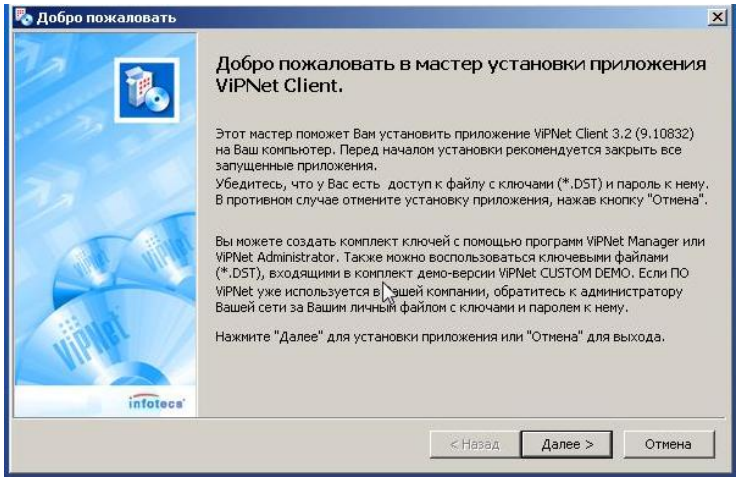


Рис. 6.82. Продолжение установки ViPNet Client

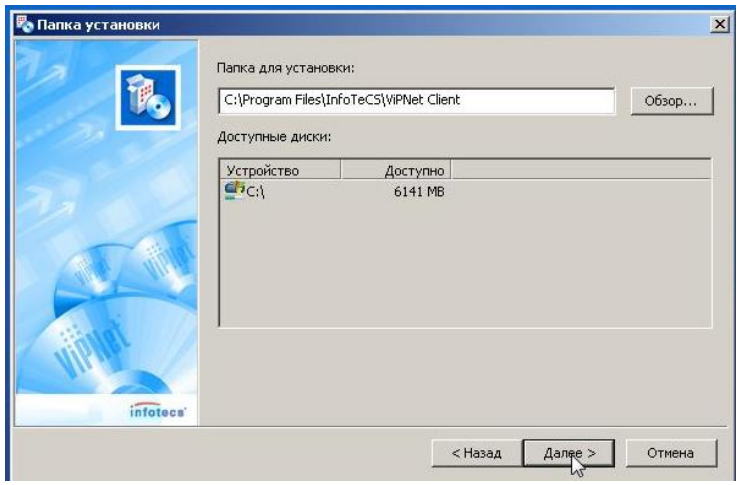


Рис. 6.83. Задание директории установки ViPNet Client

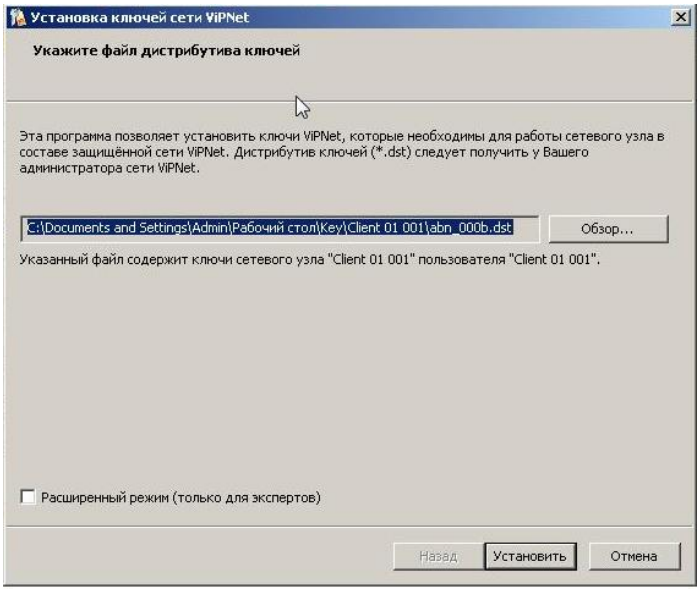


Рис. 6.84. Установка ключей сети ViPNet

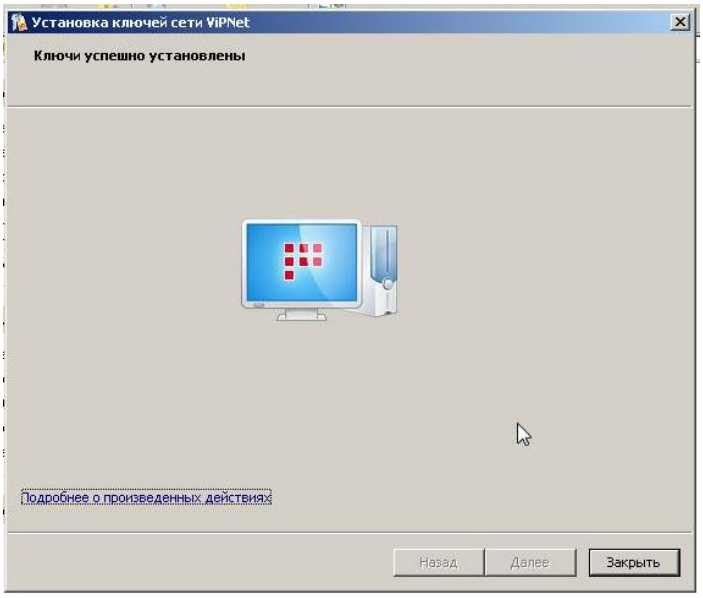


Рис. 6.85. Завершение установки ключей сети ViPNet

Установка ПО ViPNetCoordinatorна ВМ 2 описана ниже.

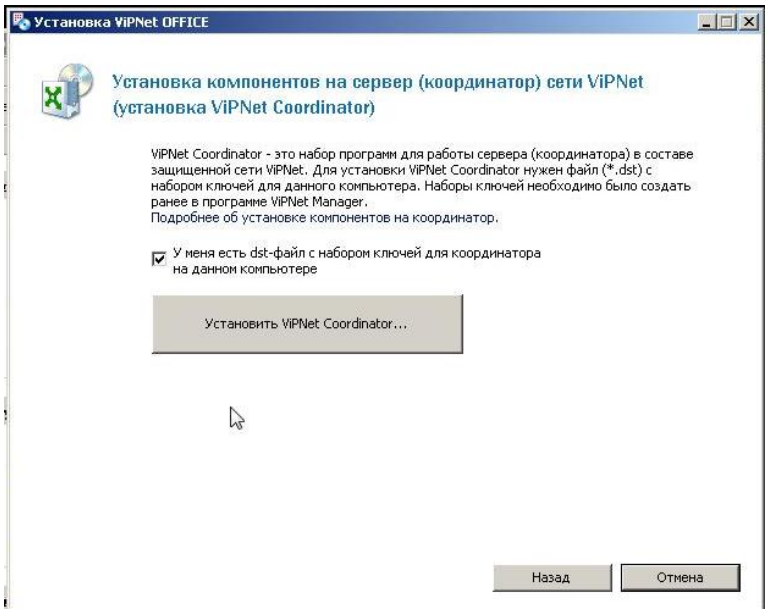


Рис. 6.86. Установка ViPNet Coordinator

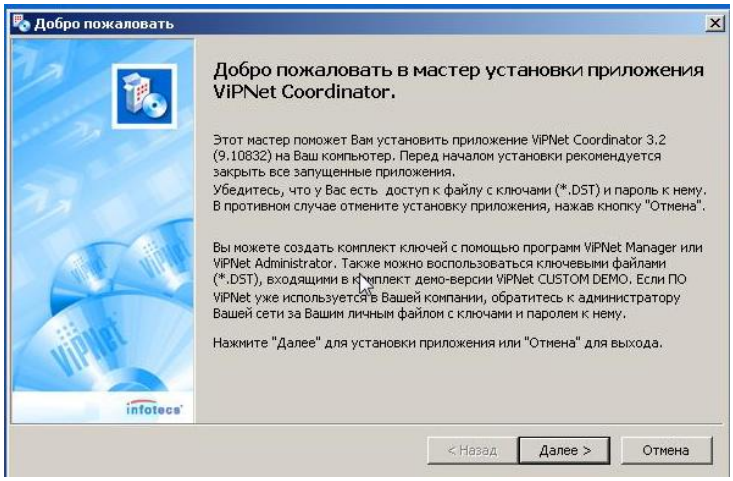


Рис. 6.87. Продолжение установки ViPNet Coordinator

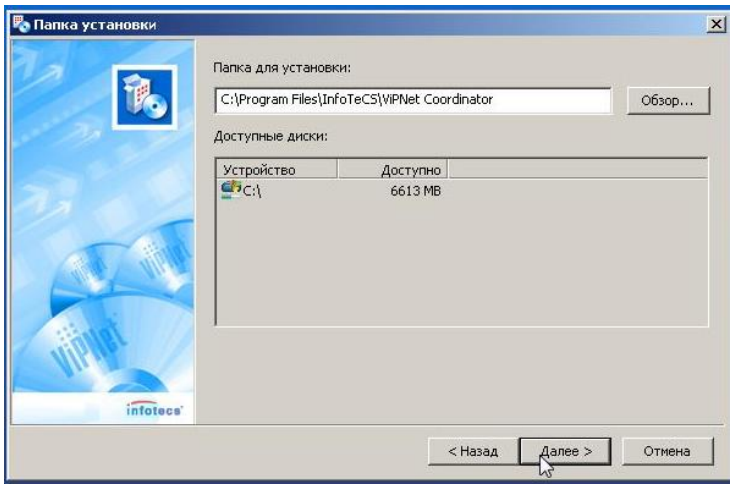


Рис. 6.88. Задание директории установки ViPNet Coordinator

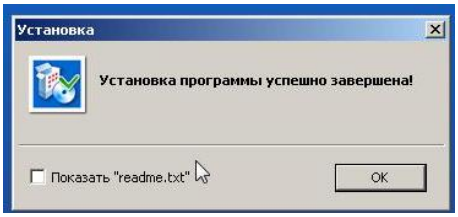


Рис. 6.89. Завершение установки ViPNet Coordinator

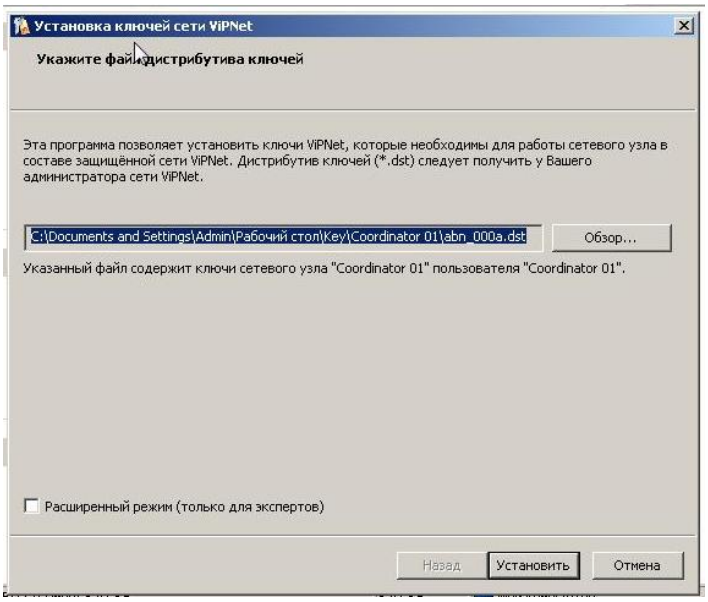


Рис. 6.90. Установка ключей для ViPNet Coordinator

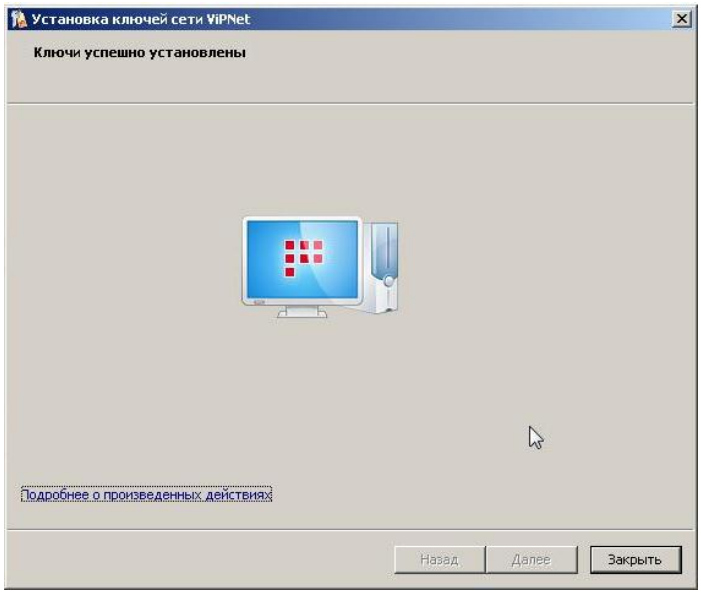


Рис. 6.91. Завершение установки ключей для ViPNet Coordinator

Очередным этапом установки ПО ViPNet является установка ViPNetClientна ВМ 3.

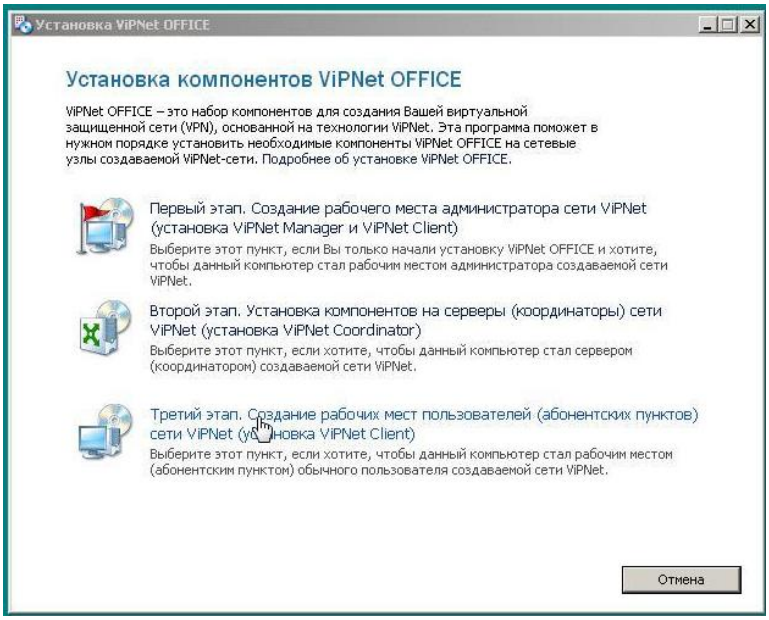


Рис. 6.92. Третий этап установки ПО ViPNet

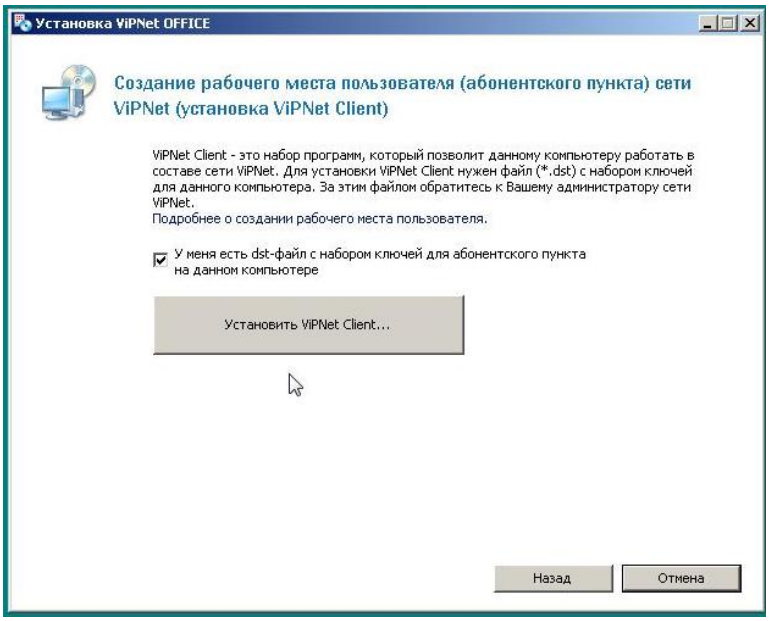


Рис. 6.93. Установка ViPNetClient

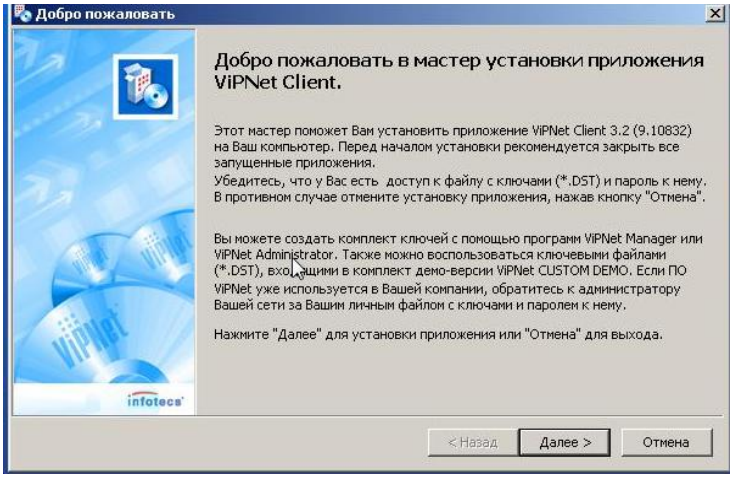


Рис. 6.94. Продолжение установки ViPNet Client

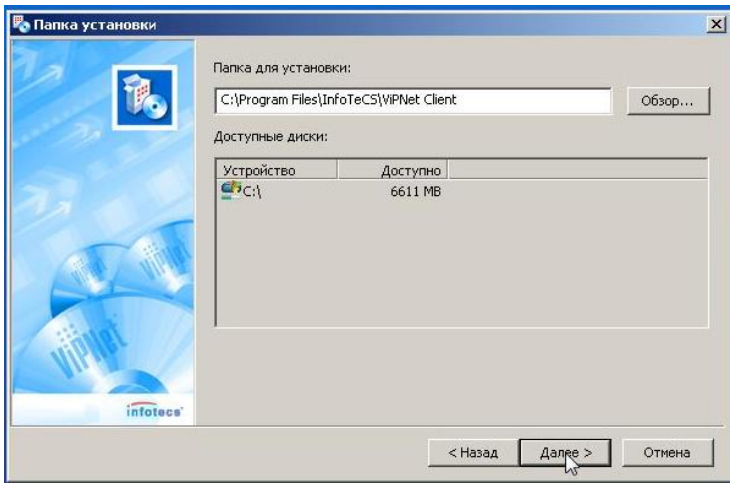


Рис. 6.95. Задание директории установки ViPNet Client

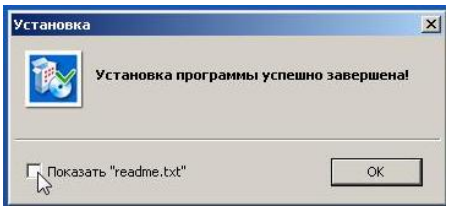


Рис. 6.96. Завершение установки ViPNet Client

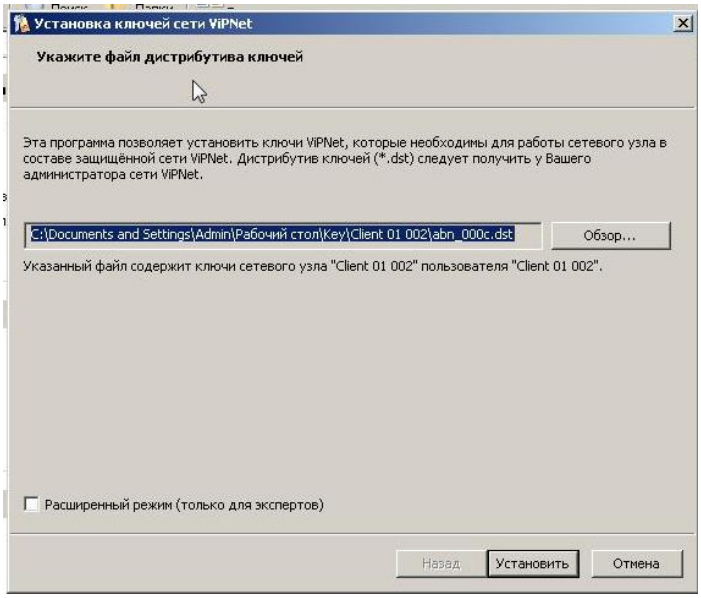


Рис. 6.97. Установка ключей для ViPNet Client

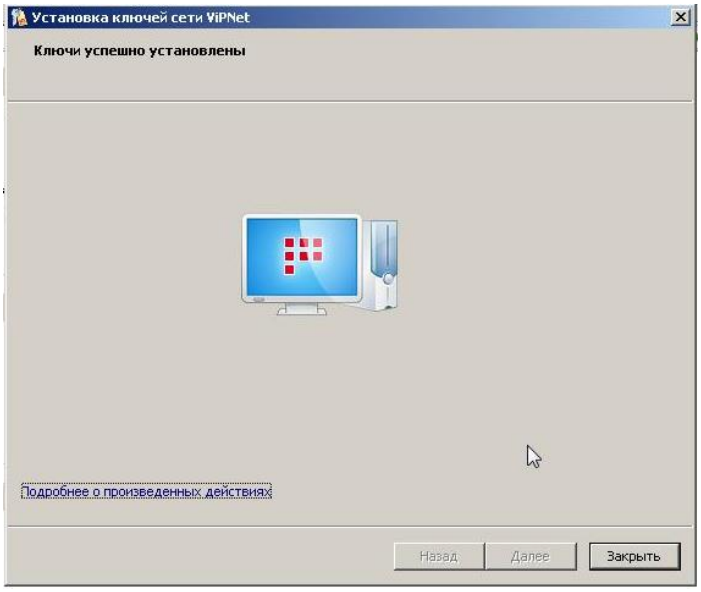


Рис. 6.98. Завершение установки ключей для ViPNet Client

Исследование защищенного сетевого взаимодействия

После установки ПО ViPNet на виртуальные машины сетевое взаимодействие становится защищенным. Для удостоверения в этом производится аналогичная процедура, что и во втором пункте испытания. По протоколу SMB передается текстовый файл Test.txt с ВМ 2 на ВМ 3. Производится захват передаваемого трафика. При этом становится видно, что захваченный трафик представлен уже не TCP-пакетами, а UDP или IPv4 (IP/241-проприетарный ViPNet протокол). При попытке выделить SMB- объект (текстовый файл test.txt)анализатор трафика таковой не обнаруживает.

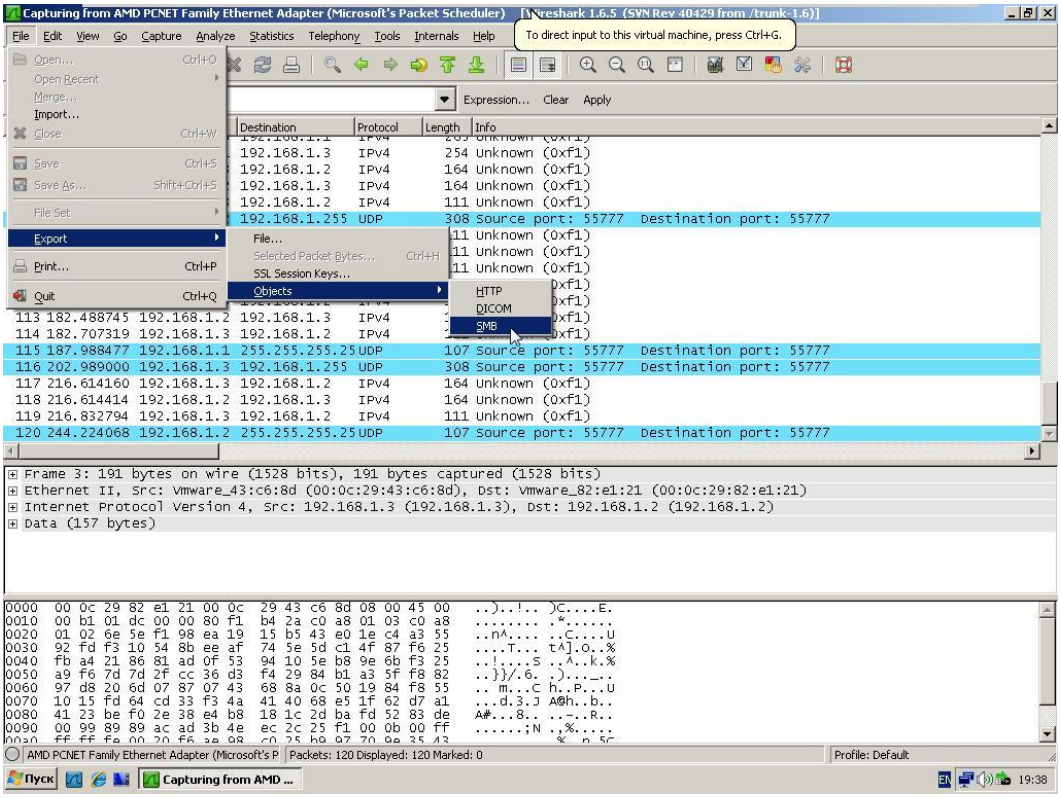


Рис. 6.99. Выделение SMB объекта

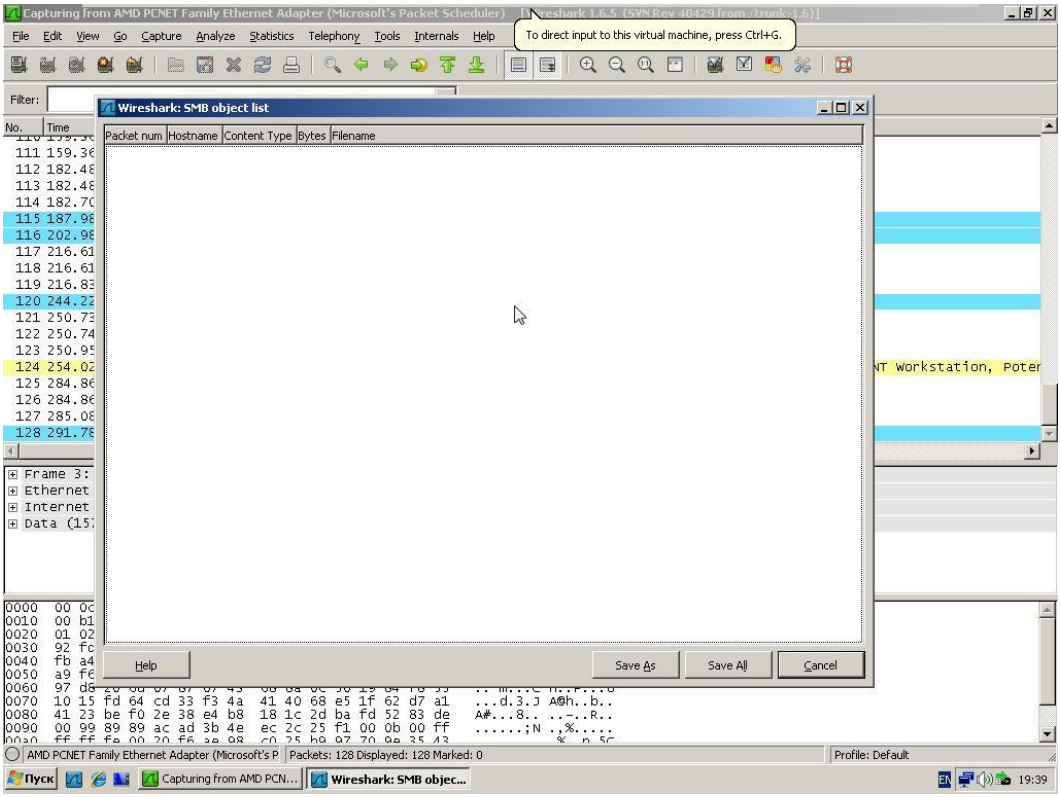


Рис. 6.100. Обнаружение SMB объекта

Аналогичным образом производится захват трафика при использовании утилиты ping на ВМ 2 для проверки связи с ВМ 3.

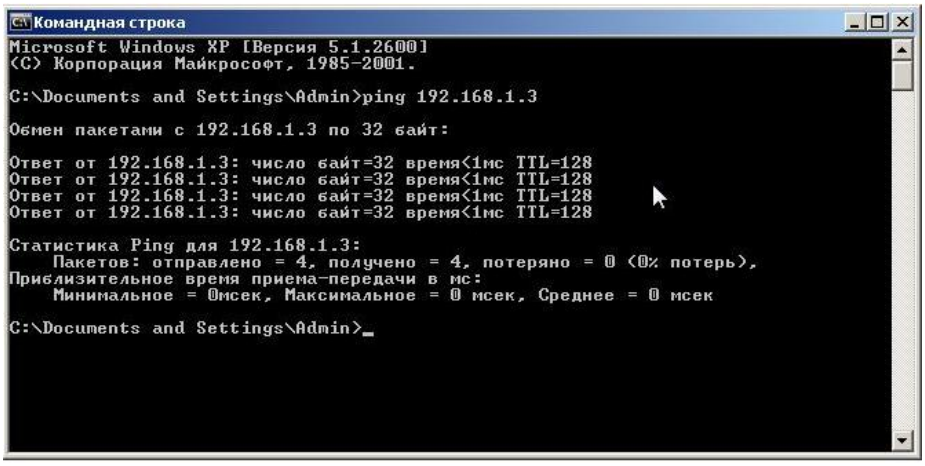


Рис. 6.101. Проверка связи с ВМ 2 с ВМ 3 с помощью утилиты ping

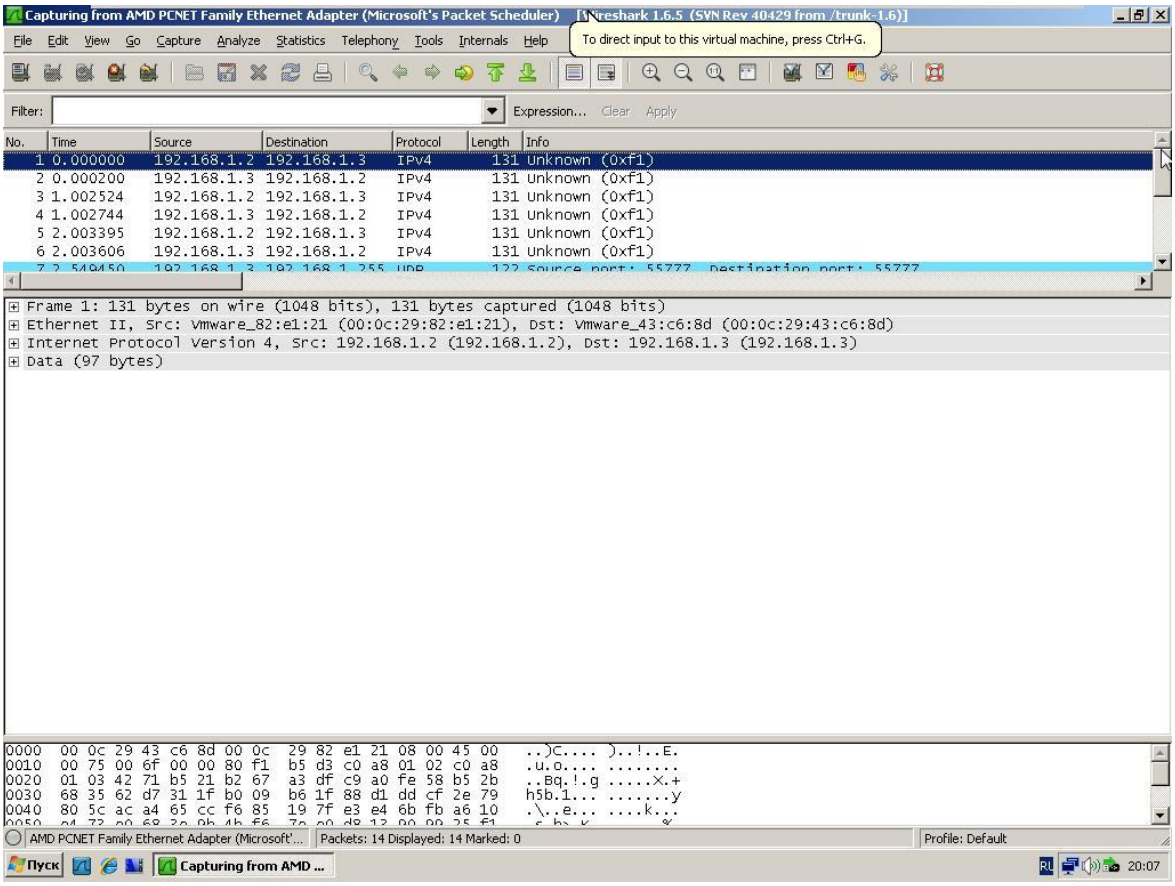


Рис. 6.102. Захваченный трафик при инициализации утилиты ping

В окне анализатора видно, что вместо ICMP-пакетов отображены IPv4-пакеты.

Было продемонстрировано испытание сетевого взаимодействия в открытом виде и в защищенном. При открытом взаимодействии не составляет труда перехватить и интерпретировать передаваемую по сети информацию. При защищенном взаимодействии, после установки ПО ViPNet, передаваемый трафик предварительно обрабатывается ViPNet-

драйвером. Он преобразует, при необходимости реальный IP-адрес отправителя в виртуальный адрес, добавляет к пакету уникальные идентификаторы узла отправителя и получателя, зашифровывает исходный IP-пакет (алгоритм ГОСТ 28147-89) и часть служебной информации, инкапсулирует исходный IP-пакет в UDP- или IP/241-пакет. В таком виде пакет отправляется в сеть, что и было обнаружено при захвате. Таким образом интерпретировать захваченную информацию не представляется возможным, так как расшифрование по алгоритму ГОСТ 28147-89, не зная ключей, практически не реализуемо.

6.3. Проектирование защищенной многоточечной видеоконференц связи на базе WEB-технологии

Цель работы: изучение и исследование принципов работы программного комплекса многоточечной видеоконференцсвязи на базе Web-технологии

Видеоконференция — это технология, которая позволяет людям видеть и слышать друг друга, обмениваться данными и совместно обрабатывать их в интерактивном режиме, используя возможности привычного всем компьютера, максимально приближая общение на расстоянии к реальному живому общению.

Видеоконференцсвязь — область информационной технологии, обеспечивающая одновременно двустороннюю передачу, обработку, преобразование и представление интерактивной информации на расстояние в режиме реального времени с помощью аппаратно-программных средств вычислительной техники двух и более пользователей.

Видеоконференция применяется как средство оперативного принятия решения в той или иной ситуации; при чрезвычайных ситуациях; для сокращения командировочных расходов в территориально распределенных организациях; повышения эффективности; проведения судебных процессов с дистанционным участием осужденных, а также как один из элементов технологий теле медицины и дистанционного обучения.

В многих государственных и коммерческих организациях видеоконференция приносит большие результаты и максимальную эффективность, а именно:

снижает время на переезды и связанные с ними расходы;

ускоряет процессы принятия решений в чрезвычайных ситуациях;

сокращает время рассмотрения дел в судах общей юрисдикции;

увеличивает производительность труда;

решает кадровые вопросы и социально-экономические ситуации;

дает возможность принимать более обоснованные решения за счёт привлечения при необходимости дополнительных экспертов;

быстро и эффективно распределяет ресурсы, и так далее.

Для общения в режиме видеоконференции абонент должен иметь терминальное устройство (кодек) видеоконференцсвязи, видеотелефон или иное средство вычислительной техники. Как правило, в комплекс устройств для видеоконференцсвязи входит:

Центральное устройство — кодек с видеокамерой и микрофоном, обеспечивающего кодирование/декодирование аудио- и видео- информации, захват и отображение контента;

устройство отображения информации и воспроизведения звука.

В качестве кодека может использоваться персональный компьютер с программным обеспечением для видеоконференций.

Большую роль в видеоконференции играют каналы связи, то есть транспортная сеть передачи данных. Для подключения к каналам связи используются сетевые протоколы IP или ISDN.

Существует два режима работы ВКС, которые позволяют проводить двусторонние (режим «точка-точка») и многосторонние (режим «многоточка») видеоконференции.

Как правило, видеоконференцсвязь в режиме «точка-точка» удовлетворяет потребности только на начальном этапе внедрения технологии, и довольно скоро возникает необходимость одновременного взаимодействия между несколькими абонентами. Такой режим работы называется «многоточечный» или многоточечной видеоконференцсвязью. Для реализации данного режима требуется наличие активации многоточечной лицензии в кодеке при условии, если устройство поддерживает данную функцию, либо специального видеосервера MCU или программно-аппаратной системы управления.

Режимы видеоконференцсвязи

Существует два основных типа видеоконференций - персональная и групповая. Персональная видеоконференция подразумевает сеанс видеосвязи, в котором участвует всего два абонента. Под групповыми же видеоконференциями подразумеваются все остальные виды видеоконференций. Различные устоявшиеся правила отображения участников видеоконференции для каждой из сторон называются видами видеоконференций.

Видеоконференция 1-на-1:

Участвуют два абонента, оба видят и слышат друг друга одновременно. Сразу оговоримся, что во время любого сеанса видеоконференции могут использоваться различные

инструменты для совместной работы, такие как обмен текстовыми сообщениями, файлами, презентациями и прочими медиаданными.

Рис. 6.103. Структура видеоконференции «1 на 1»

Симметричная видеоконференция

Она же видеоконференция с постоянным присутствием. Так называют сеанс видеоконференции, в котором участвуют более 2 человек и все участники видят и слышат друг друга одновременно. Естественно, видеоконференция подразумевает полнодуплексное общение. Другими словами, это аналог круглого стола, где у всех равные права. Групповая видеоконференция подходит для встреч, где требуется максимальная вовлеченность каждого участника.

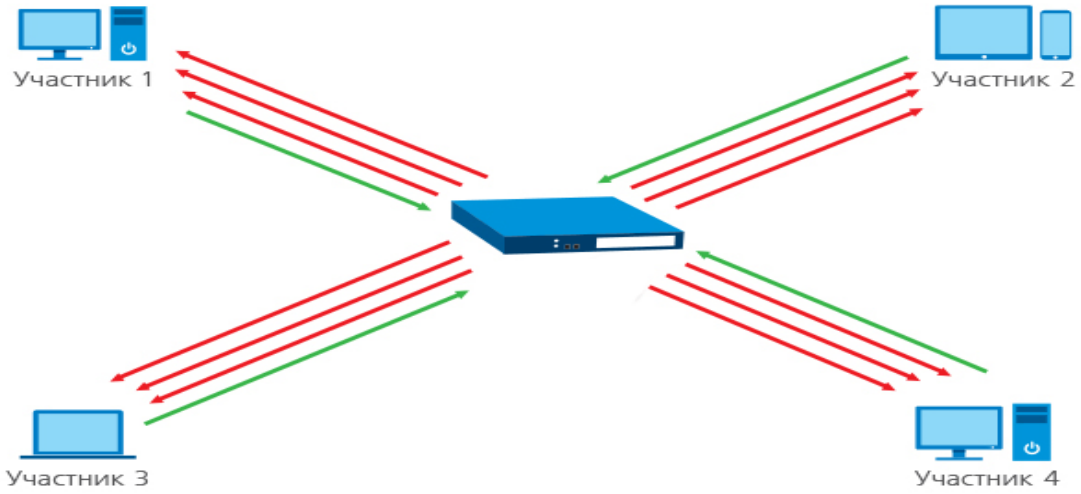


Рис. 6.104. Структура «симметричной» видеоконференции

Видеоконференция с активацией по голосу

Название такого режима пошло от английского обозначения Voice Activated Switching (VAS). Эта видеоконференция предполагает следующий формат общения: все участники сеанса слышат и видят на своих экранах только выступающего докладчика, в то время как он сам видит себя либо предыдущего оратора. Возможны небольшие вариации данного механизма, но суть остаётся следующей: сервер ВКС отслеживает голосовую активность абонентов и переключает транслируемое всем участников изображение на говорящего. У данного режима есть существенные недостатки, например, ложные срабатывания на шум, кашель или звонок мобильного телефона.

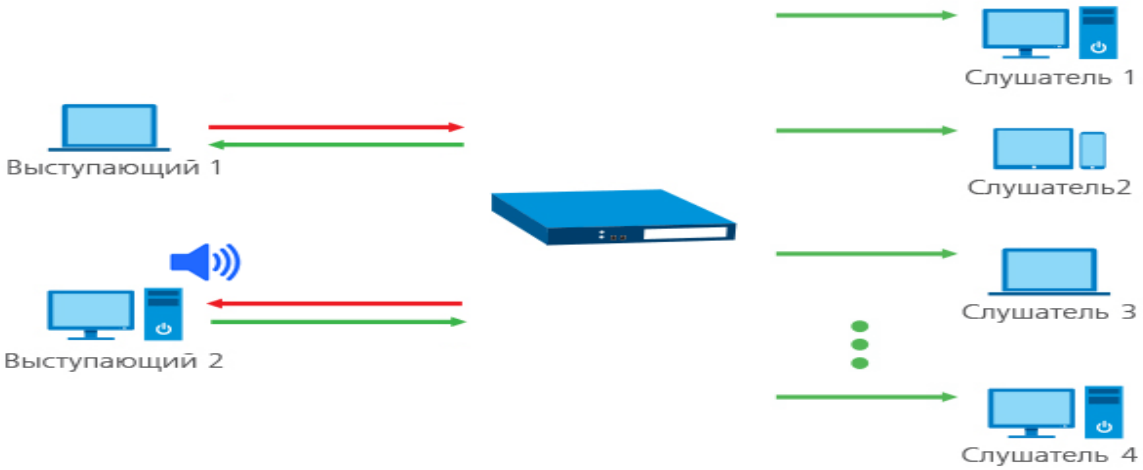


Рис. 6.105. Структура видеоконференции «с активацией по голосу»

Селекторная видеоконференция

Режим в котором участники делятся на два вида: докладчики и слушатели, где каждый из слушателей может стать докладчиком (с разрешения организатора конференции). Ведущий такой конференции сам назначает докладчиков и может удалить их с видео-трибуны в любой момент.

Этот режим может так же называться ролевой видеоконференцией. Селекторная видеоконференция используется чаще всего при проведении веб-конференций (вебинаров).

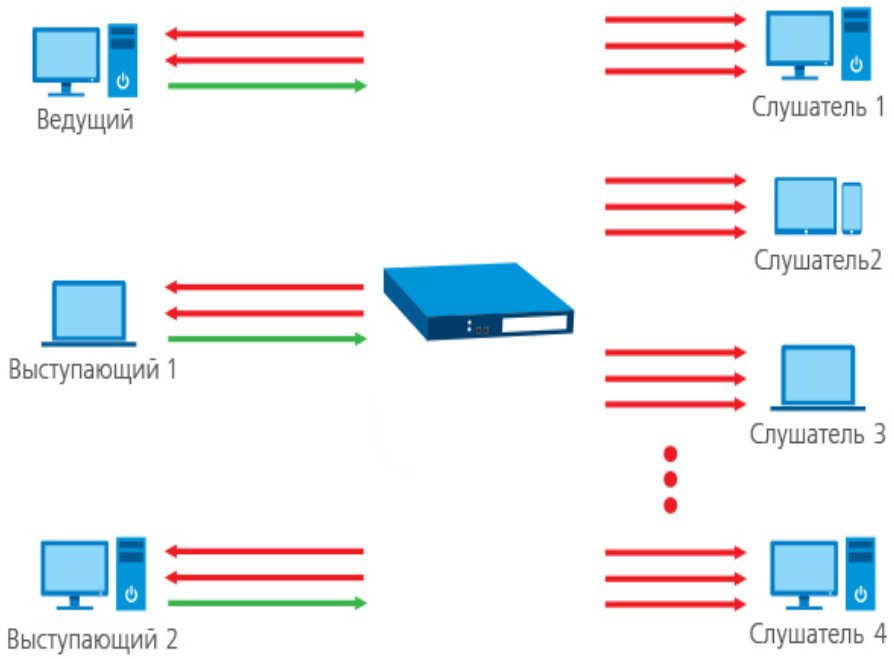


Рис. 6.106. Структура «селекторной» видеокнференции

Видеоконференция для дистанционного образования

Специальный режим "Видеоурок", в котором что все участники(ученики) будут видеть и слышать только одного вещающего(преподавателя), а он будет видеть и слышать всех участников видеоконференции. То есть, ученики не имеют обратной связи между собой.

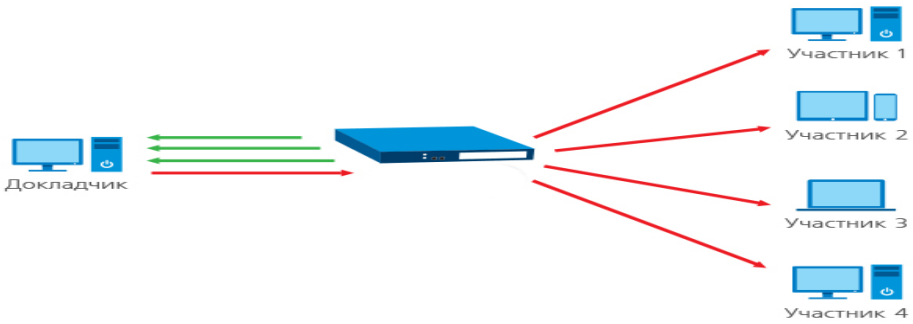


Рис. 6.107. Структура видеоконференции «для дистанционного образования»

Видеотрансляция

Вид видеоконференции, в котором докладчик вещает на широкую аудиторию слушателей, при этом он не видит и не слышит их. Остальные участники видят и слышат только докладчика. Обратная связь возможна только через текстовый чат.

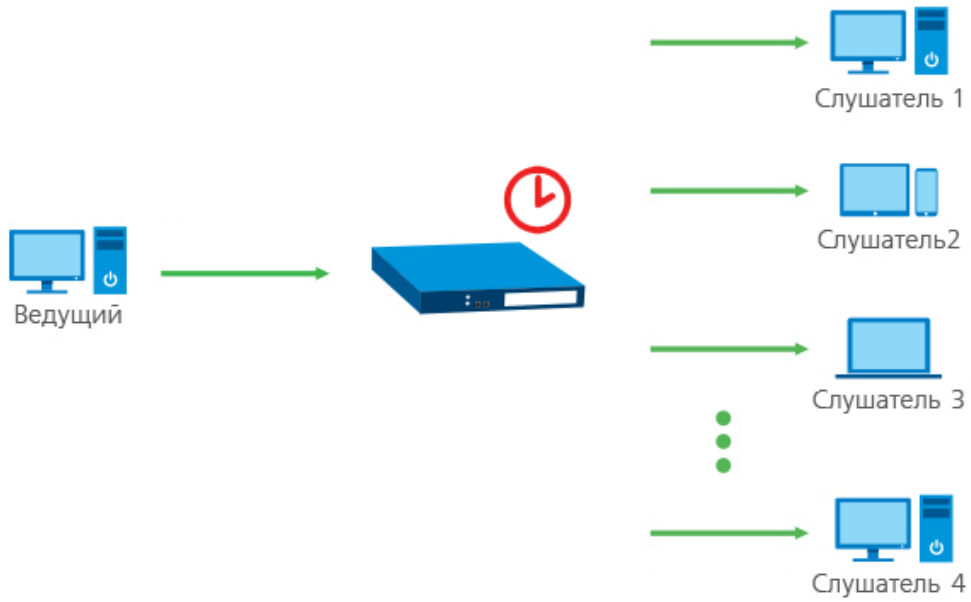


Рис. 6.108. Структура «видеотрансляции»

Организация видеосвязи для различных каналов связи

По локальной сети:

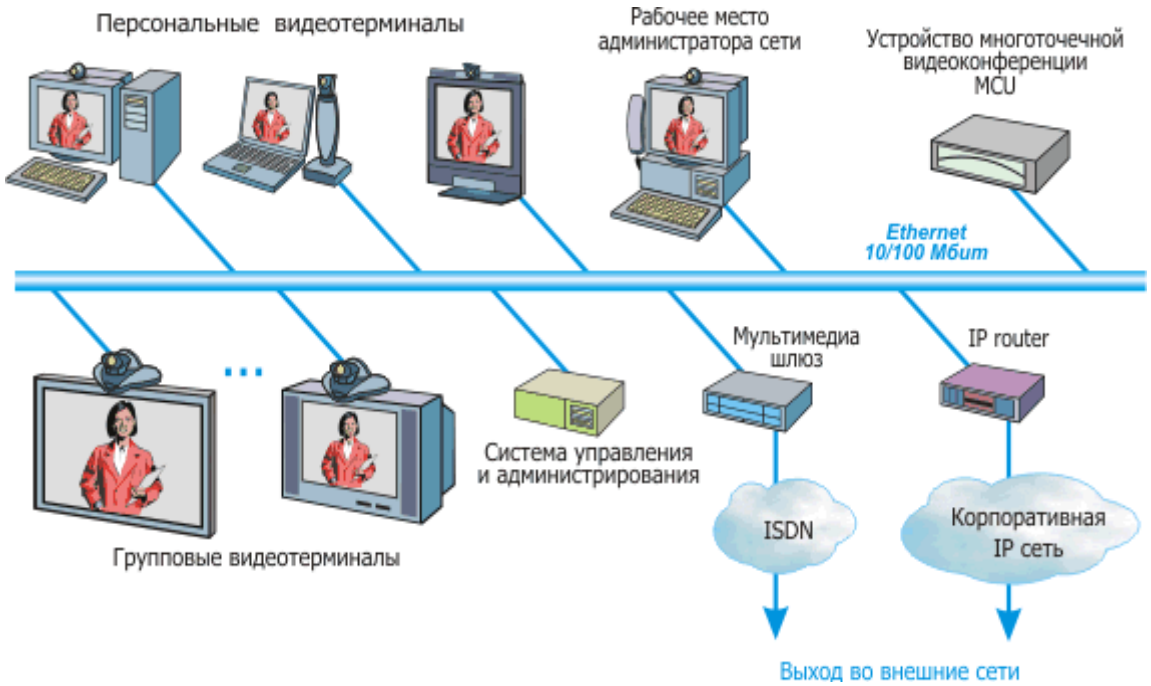


Рис. 6.109. Структурная схема многоточечной видеоконференции в локальной сети.

В сети Интернет:

Самый простой и дешевый метод организации видеоконференцсвязи через Интернет. Для организации видеоконференцсвязи через Интернет требуется иметь статические IP-адреса и

каналы связи с пропускной способностью не менее 512 кБит/св обе стороны (для исходящего и входящего трафика).

Основным недостатком систем КВКС в Интернет можно считать существенную зависимость качества видео- и аудиопотоков от загрузки сети. В проведенных экспериментах качество аудиопотока изменялось от близкого к качеству звука при телефонном разговоре до плохого, при котором наблюдались прерывания звука. Передача видеопотоков в условиях недостаточной пропускной способности канала сопровождалась уменьшением числа передаваемых кадров в секунду с 8-10 до 1-2, мозаичностью передаваемого подвижного изображения. Тем не менее в условиях неудовлетворительного качества звука интерактивность может эффективно поддерживаться путем обмена текстовыми сообщениями в режиме on-line, а надежный режим обмена данными (в первую очередь, приложения Whiteboard и Filetransfer) позволяет считать такие системы достаточно эффективным средством поддержки процесса обучения в среде Интернет.

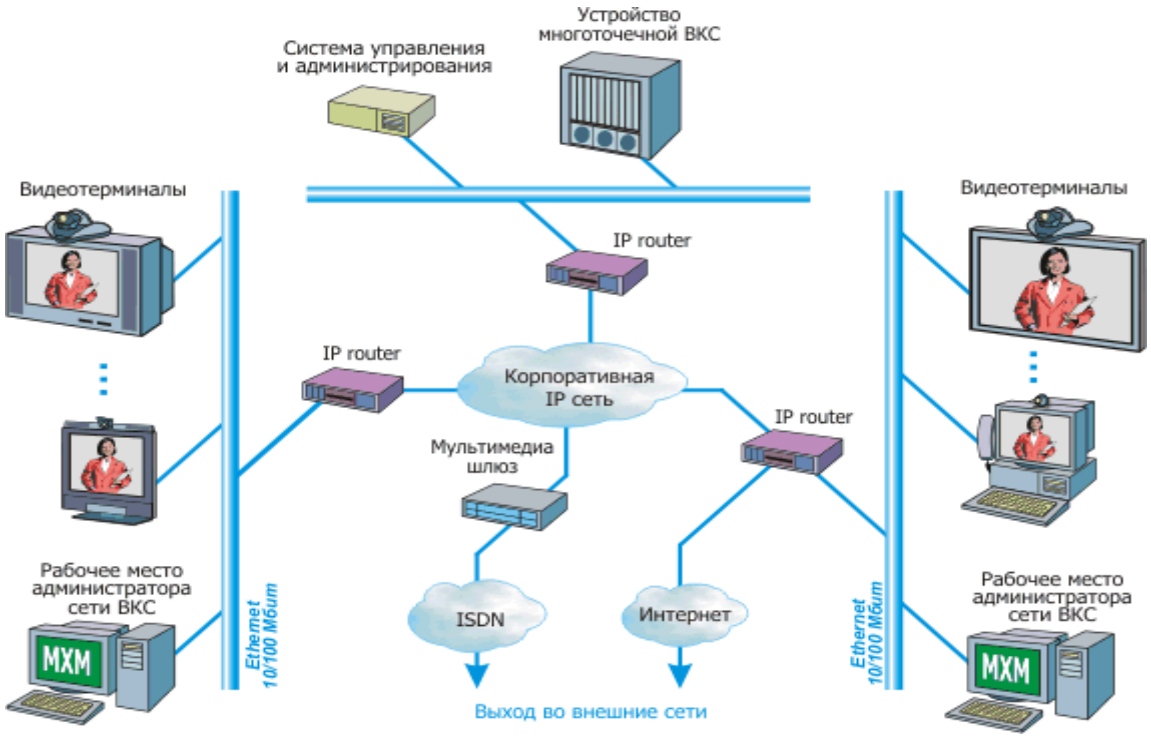


Рис. 6.110. Структурная схема многоточечной видеоконференциивтерриториально распределенной IP-сети.

По протоколу ISDN:

Аббревиатура ISDN расшифровывается как цифровая сеть с интеграцией услуг. Цифровые сети с интегральными услугами относятся к сетям, в которых основным режимом связи является режим коммутации каналов, а данные обрабатываются в цифровой форме.

Необходимо отметить, что ISDN имеет ряд преимуществ по сравнению с традиционными аналоговыми сетями, но вот по сравнению с новыми телекоммуникационными технологиями передачи данных имеет ряд критичных недостатков:

тяжело отследить, на каком участке произошел сбой связи;

низкая оперативность восстановления каналов связи;

небольшая распространенность на территории РФ;

всего несколько операторов связи поддерживают данную технологию;

сравнительно высокая стоимость применения услуги связи при межрегиональном соединении.

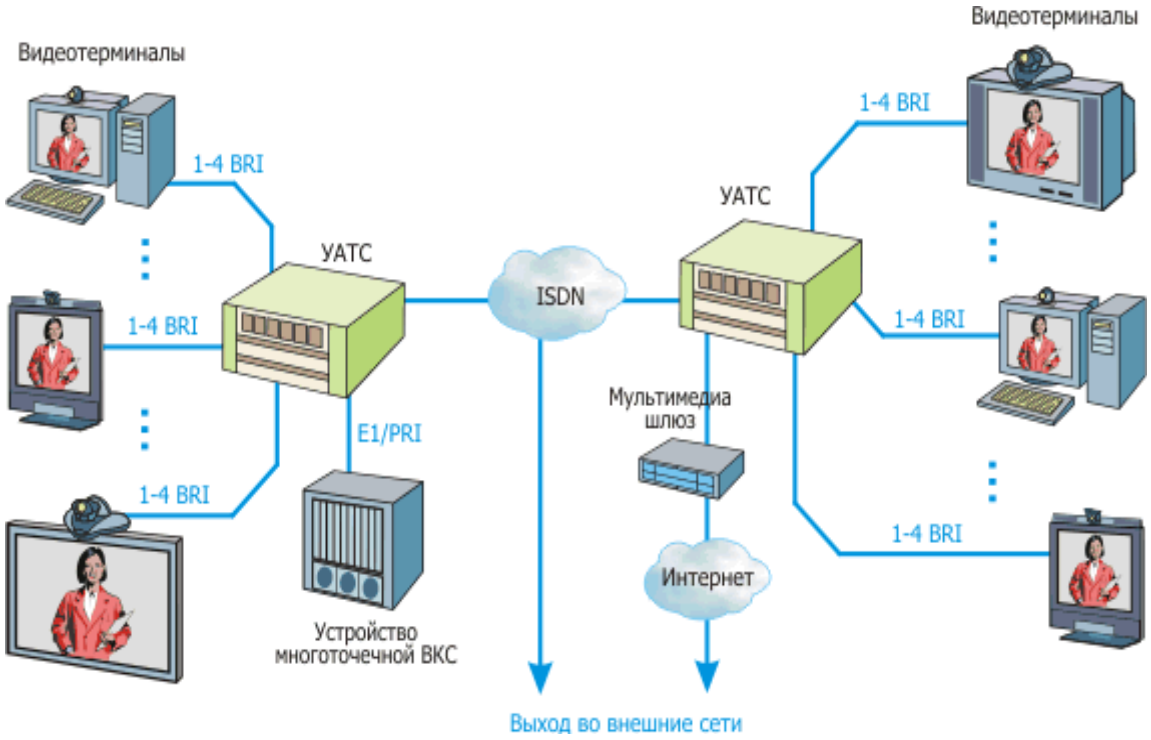


Рис. 6.111. Структурная схема многоточечной видеоконференции ISDN.

Современные методы и средства управления в сетях видеоконференцсвязи

Для любой информационной сети — телефонной, вычислительной и т.д. можно сформулировать общий принцип: чем она больше, тем сложнее в управлении. Не являются исключением из этого правила и сети видеоконференцсвязи (ВКС), более того, если в общие задачи управления сетями обычно не включается требование управления оборудованием, установленным на рабочих местах пользователей, то для сетей ВКС это становится одной из основных функций. Ситуация осложняется тем, что современная архитектура сетей ВКС требует высокой работоспособности от гетерогенных решений, построенных с использованием разнородных технологий на основе оборудования разных производителей.

Для обеспечения безопасности и повышения надежности вычислительных сетей используются технологии, получившие название управления сетями — наблюдение за функционированием, тестирование, предотвращение, выявление и устранение сбоев, обеспечение функционирования сетевых сервисов с задаваемым качеством обслуживания.

Принятые рекомендации МСЭ-Т X.700 и близкий к ним стандарт ISO/IEC 7498-4 ввели концептуальную модель управления сетями. Задачи систем управления сетями в них разбиваются на пять функциональных групп: обработка ошибок (fault management), управление конфигурацией (configuration management), учет (accounting management), управление производительностью (performance management), управление безопасностью (security management). Все они объединяются под общим названием FCAPS.

Применительно к сетям видеоконференцсвязи задачи, предусмотренные моделью управления, должны включать в себя следующие функции:

Обработка ошибок — обеспечение администратора сети необходимыми инструментами для обнаружения сбоев и отказов сетевых и терминальных устройств ВКС, определения их причин и принятия действий по восстановлению. Для этого предоставляются механизмы: уведомления о сбоях; регистрации ошибок и ведения журнала; анализа сообщений об ошибках и выявление их источника; проведения диагностического тестирования; коррекции и восстановления от сбоев (по возможности в автоматическом режиме); резервирования и оперативного подключения ресурсов сети.

Управление конфигурацией — отслеживание и настройка конфигурации сетевого программного и аппаратного обеспечения (настройки и состояние отдельных сетевых устройств и сети в целом). Может предоставляться функциональность по инициализации, реконфигурации, модернизации программного обеспечения, запуску и отключению управляемых устройств. Сюда же включаются механизмы обеспечения единого плана нумерации.

Учет — измерение использования и доступности сетевых ресурсов для: учета имеющихся сетевых ресурсов; экономического учета (выставление счетов и т. п.); управления пользователями (учет использования сети в разрезе отдельных пользователей и групп).

Управление производительностью — измерение производительности сети, сбор и анализ статистической информации о поведении сети для ее поддержания на приемлемом уровне как для оперативного управления, так и для планирования ее развития. Управление производительностью предоставляет возможность: получить уровень загрузки и ошибок сетевых устройств;

обеспечивать соответствующий уровень производительности за счет необходимых сетевых ресурсов.

Управление безопасностью — контроль доступа к оборудованию и сетевым ресурсам (с ведением журналов доступа), предотвращение, обнаружение и пресечение несанкционированного доступа.

Открытый сервер видеоконференций OpenMeetings

OpenMeetings - это серверное программное обеспечение с открытым исходным кодом (Open Sorce), предназначенное для проведения вебконференций.

OpenMeetings позволяет мгновенно создать конференцию в Интернете, для участия в которой нужен лишь браузер. В OpenMeetings можно использовать микрофон и веб-камеру, делиться документами и экраном, рисовать на белой доске, приглашать участников по e-mail, записывать встречи. Можно также создавать опросы и голосовать по ходу встречи. Для модератора OpenMeetings предоставляет полный контроль над возможностями пользователей. Так что OpenMeetings вполне подойдет для в школ, университетов и других учебных заведений.

OpenMeetings доступен как готовый веб-сервис на сайте разработчика, но за определенную плату. Здесь же можно бесплатно зарегистрироваться и испытать его.

Чтобы использовать OpenMeetings бесплатно, и при этом безо всяких ограничений и контрибуций, нужно загрузить инсталляционный пакет, и установить его на веб-сервере своего учебного заведения (установка OpenMeetings).

Пользователь OpenMeetings должен зарегистрироваться на сервере. Общение происходит в различных комнатах для встреч, в которых различные группы могут настроить свои отдельные режимы работы видео, списки участников, возможности обмена информацией и политики безопасности.

Презентации с экрана OpenMeetings можно загрузить на свой ПК, в том числе в формате PDF, причем с очень хорошим качеством. В этом смысле OpenMeetings очень подходит для конвертирования презентаций из PPT в PDF. Видеозапись конференции можно сохранить в формате AVI / FLV. Есть чат и личные сообщения. Имеется календарь с системой уведомлений (электронная почта или Ical). Возможна интеграция с Moodle, Joomla, Wordpress, Drupal и другими популярными LMS и CMS.

Порядок установки OpenMeetings

Устанавливаем вспомогательные пакеты необходимые для работы Openmeeting:

1. Запустить flashplayer10_1_p3_plugin_022310.exe, нажать установка
2. Запустить ImageMagick-6.6.0-0-Q16-windows-dll.exe, нажать «Next», «Next», «Next»

3. Запустить установку пакета OOo_3.2.0_Win32Intel_install_wJRE_ru.exe (OpenOffice), выбирайте полную установку. В том числе установится Java JDK 1.6 необходимая для работы openview.

4. Создать папку ffmpeg в например и скопировать туда файл ffmpeg.exe

5. Распаковать sox-14.3.0-win32.zip в например .

6. Установить Postgres и создать базу Openmeetings

7. Распаковываем openmeetings_1_1_r2905.zip и запускаем red5.bat

8. Копируем \webapps\openmeetings\conf\postgres_hibernate.cfg.xml в \webapps\openmeetings\conf\hibernate.cfg.xml

9. Редактируем файл \webapps\openmeetings\conf\hibernate.cfg.xml, указываем параметры авторизации СУБД.

10. Создаем переменную окружение JAVA_PATH с путем до java, в нашем случае «C:\Program Files(x86)\Java\jre6

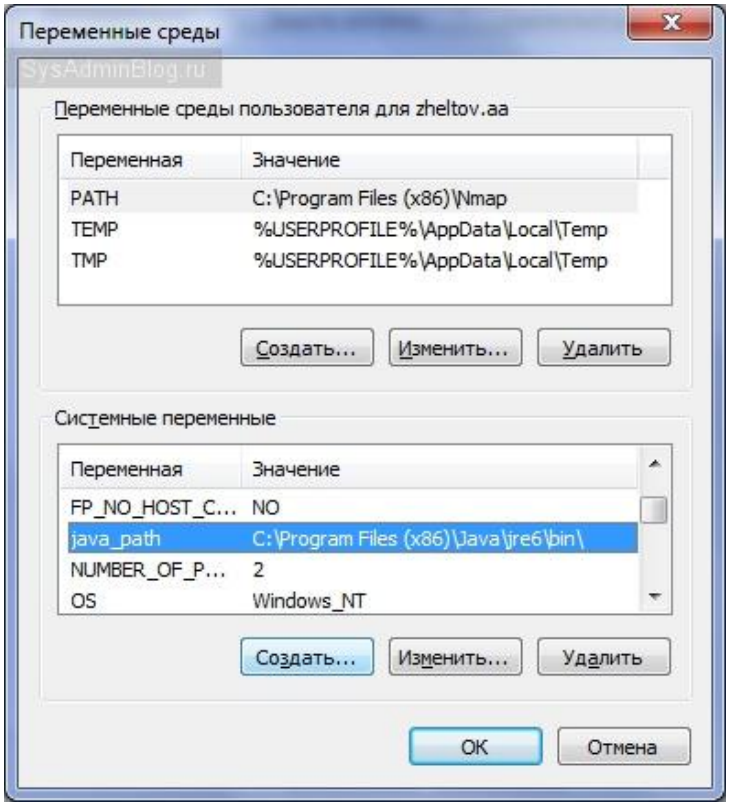


Рис. 6.112. Окно переменных сред

11. Перегружаем сервер

12. Открываем адрес http://servername:5080/openmeetings/install

13. Указываем свои настройки и пути до установленных пакетов swftools, ffmpeg, ImageMagick, sox и жмем Install.

Если предустановка выполнена правильно, при открытии адреса выведется следующее:

Рисунок 6.113. Установка OpenMeetings (шаг 1)

Ввод данных представлен на рисунке 6.114

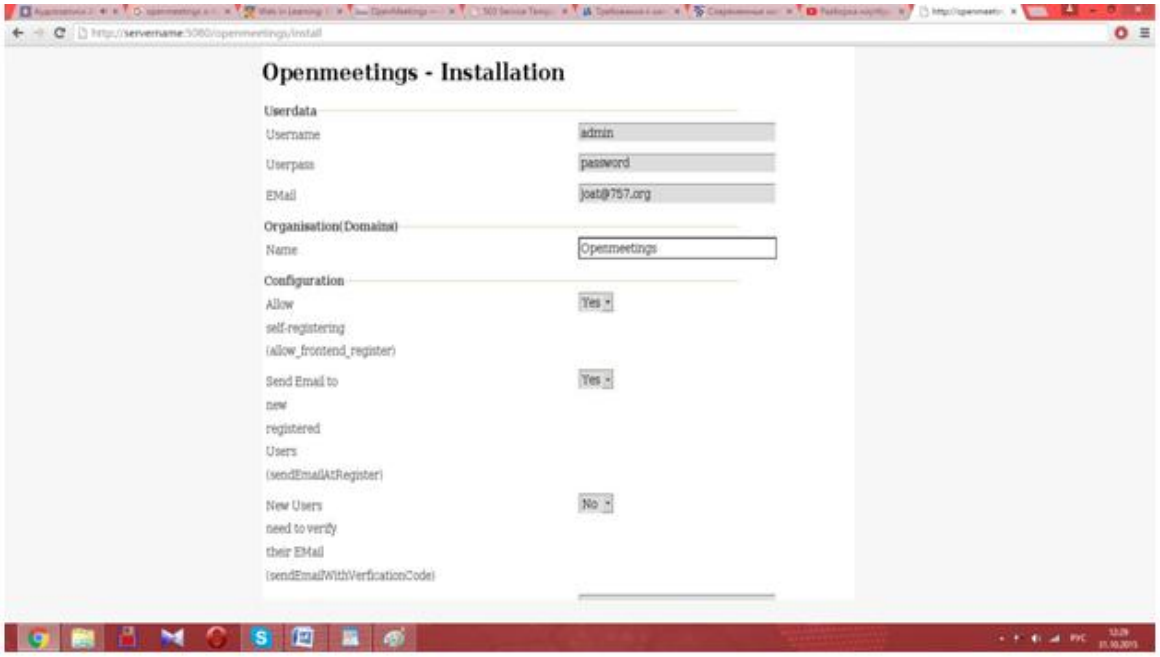


Рис. 6.114. Установка OpenMeetings (шаг 2)

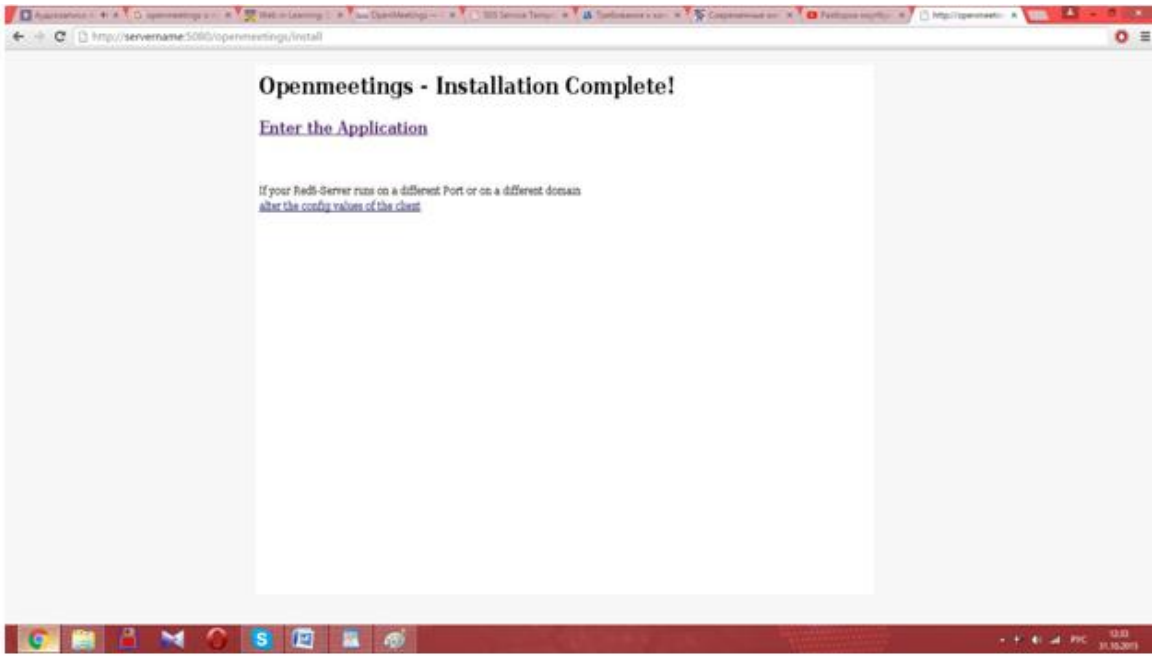


Рис. 6.115. Установка OpenMeetings выполнена

Авторизация представлена на рисунке 6.116

Рис. 6.116. Авторизация OpenMeetings

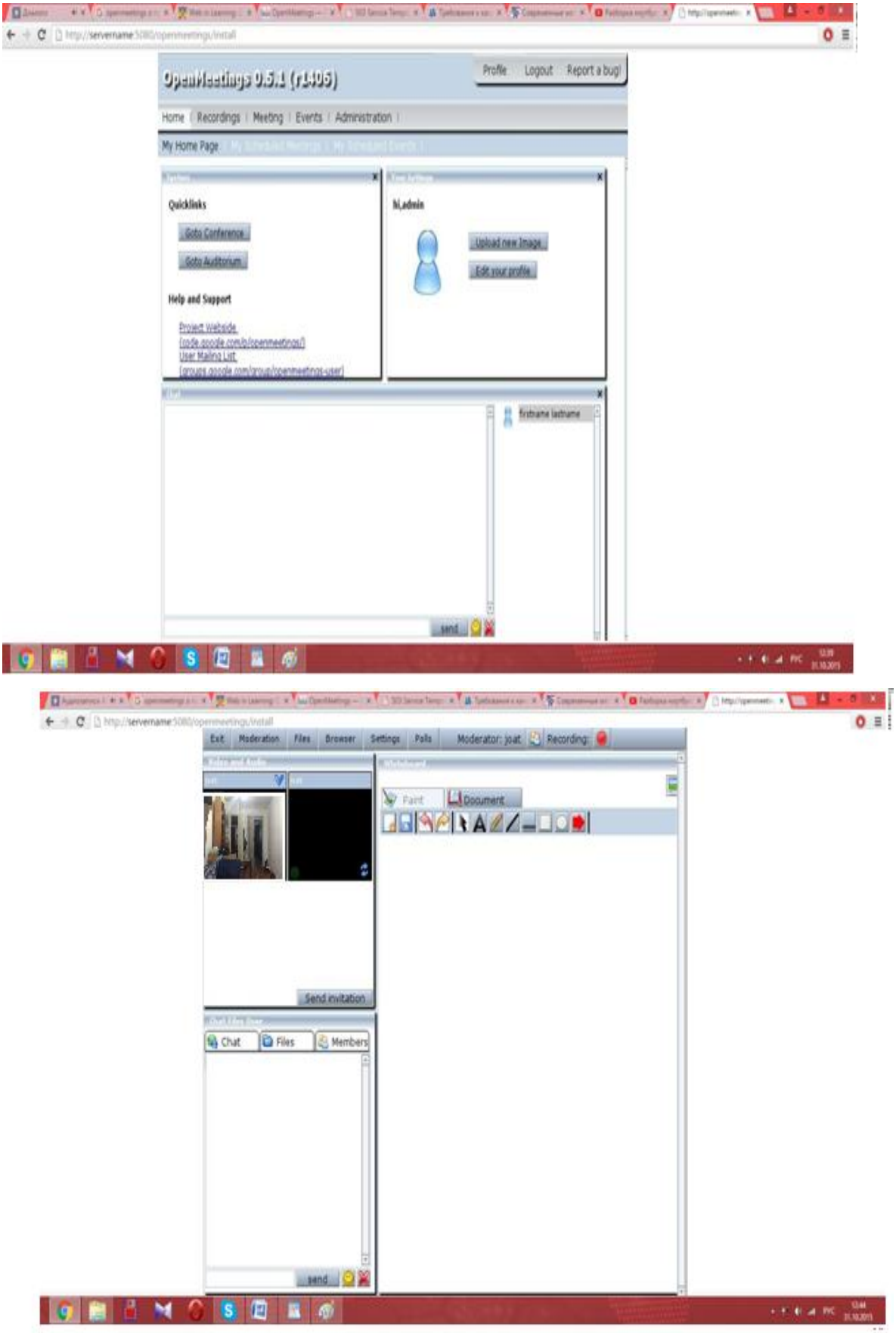


Рис. 6.117. Рабочий интерфейс программы

Требования к использованию системы видеоконференций:

Для полноценной возможности использовать видеоконференции необходимо:

Веб-Камера, подключённая и настроенная

Микрофон

Наличие динамиков.

При входе в систему будет предложено авторезироваться, либо зарегистрироваться, если вы этого еще не сделали. Окно входа в систему представлено на рисунке 2.118

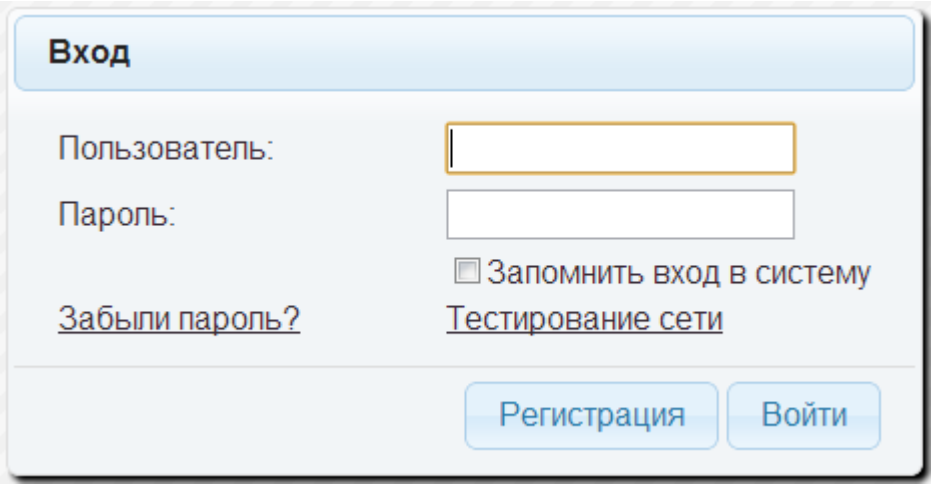


Рис. 6.118. Окно авторизации.

Если нажать кнопку «Регистрация» появится форма представленная на рисунке 2.119, где необходимо ввести требуемые учетные данные.

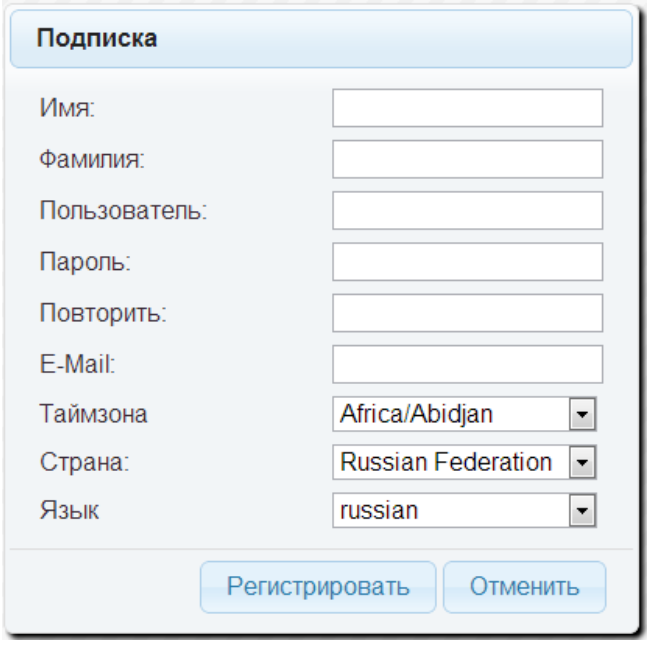


Рис. 6.119. Форма регистрации

После авторизации появляется основное командное окно, представленное на рисунке 6.121

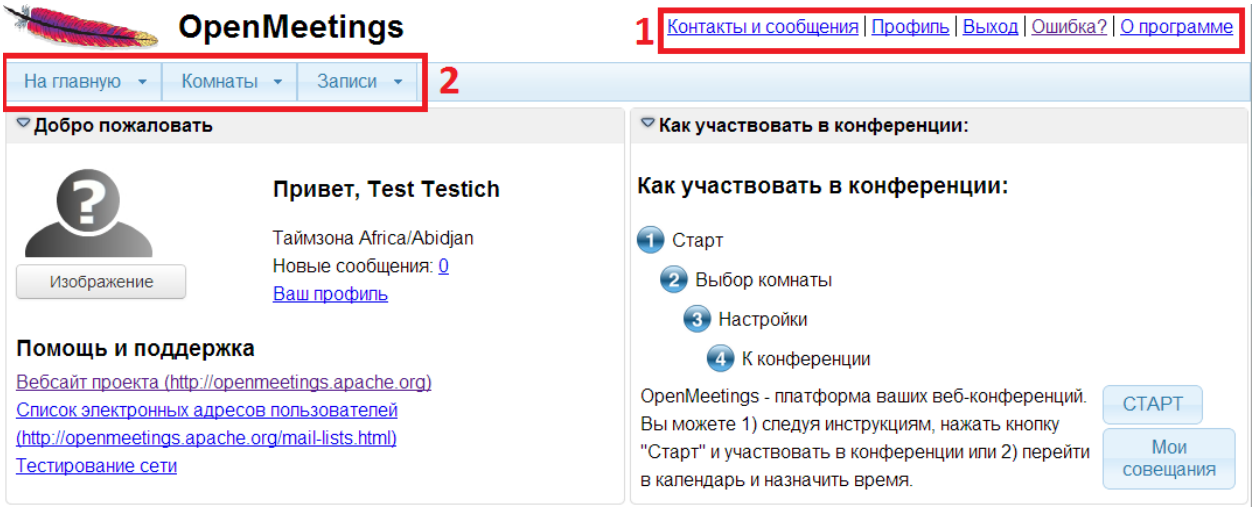


Рис. 6.120. Основное командное окно

Содержит две основные панели.

Первая панель:

Контакты и сообщения – будут отображаться ваши личные сообщения

Профиль – редактирование ваших личных данных

Выход – выйти из текущего пользователя

Ошибка? – сообщить об ошибке

О программе – о программе

Вторая панель:

На главную

Моя домашняя страница – возращение на главную страницу

Мои совещания – календарь с предстоящими совещаниями

Комнаты

Публичные комнаты – публичные комнаты, которые доступны для всех

Приватные комнаты – комнаты, которыми могут пользоваться пользователи из той же группы

Мои комнаты – комнаты предназначенные для персонального использования.

Записи

Записи – просмотр записей прошедших конференций

Так же можно изменить свой профиль и использовать поиск пользователей, скриншоты представлены на рисунках 6.121, 6.122.

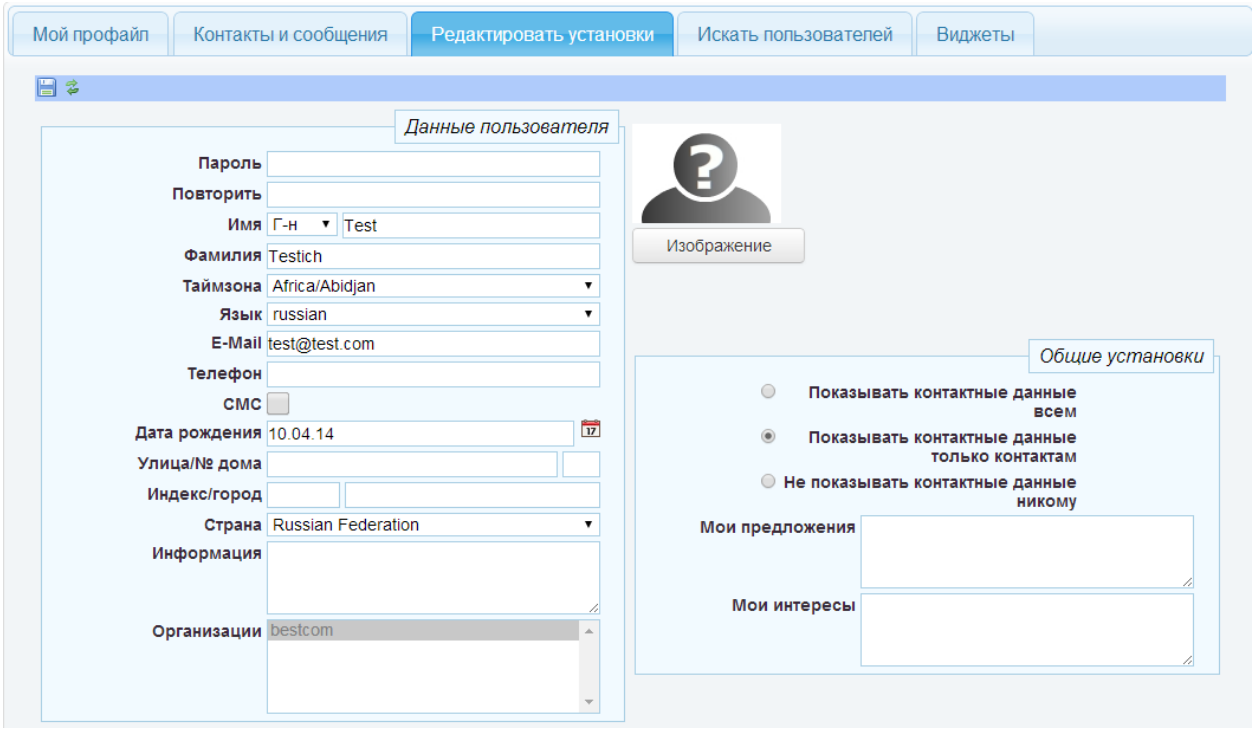


Рис. 6.121. Окно изменение учетной записи

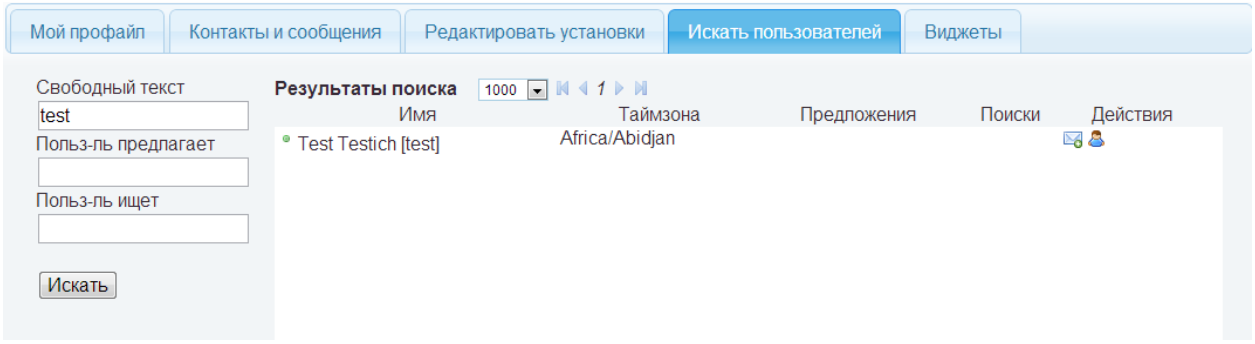


Рис. 6.122. Окно поиска пользователей

Вход в комнату конференции производиться следующим образом: нажимается кнопка «комнаты» и после выхода контекстного меню выбирается тип комнаты (приватные, публичные, мои), как представлено на рисунке 6.123

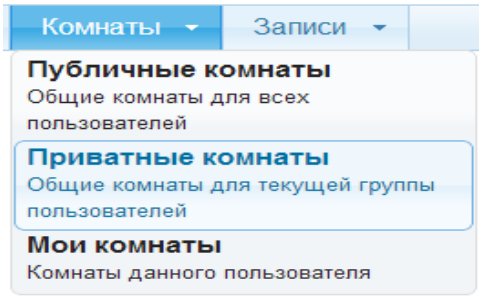


Рис. 6.123. Окно выбора типа комнат

После выбора высветится список всех доступных комнат с их описанием и количеством участников в конференции.

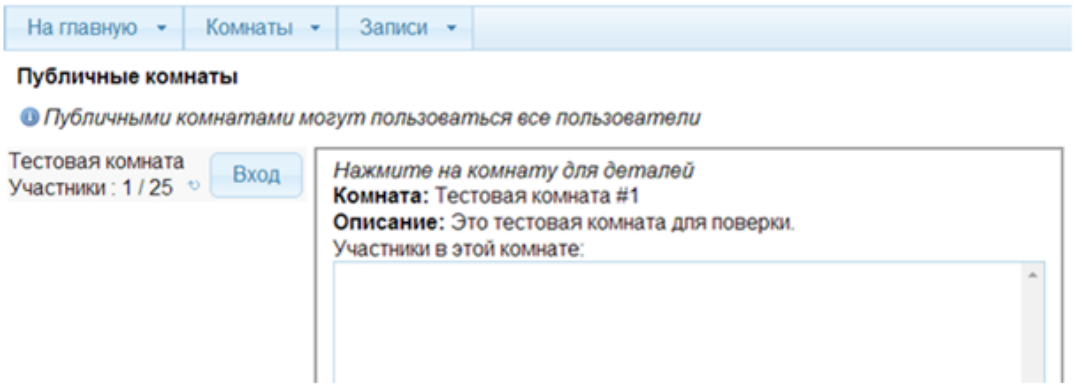


Рис. 6.124. Комната конференции

На рисунке 6.125 представлен скриншот окна конференции.

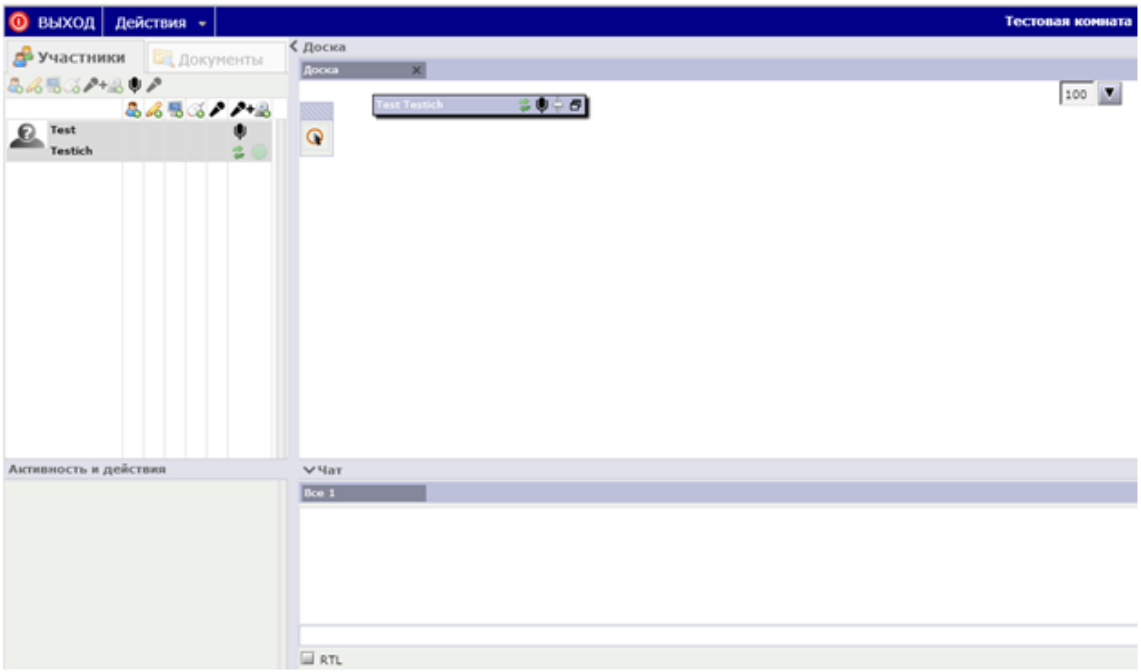


Рис. 6.125. Окно конференции

Слева представлен список участников конференции, а так же их права в данной конференции.

Наличие либо отсутствие определённых типов прав можно определить по зелёным галочкам в соответствующем столбце напротив участника конференции.

Также в нижней части окна представлена панель для Чата, что позволяет быстро обмениваться сообщениями со всеми участниками конференции

В результате проделанной работы было изучена теория построения видеоконференцсвязи, а так же установлен и исследован открытый сервер видеоконференций OpenMeetings.

С ростом технологий и развитием малого и крупного бизнеса, все актуальней становится использование многоточечной видеоконференцсвязи.

ЧАСТЬ 2. МУЛЬТИСЕРВИСНЫЕ СИСТЕМЫ И СЕТИ СВЯЗИ

7. СИСТЕМЫ МОБИЛЬНОЙ РАДИОСВЯЗИ

7.1. истемы мобильной связи стандарта GSM

GSM относится к сетям второго поколения (2 Generation) (1G — аналоговая сотовая связь, 2G — цифровая сотовая связь, 3G — широкополосная цифровая сотовая связь, коммутируемая многоцелевыми компьютерными сетями, в том числе Интернет).

Мобильные телефоны выпускаются с поддержкой 4 частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц.

В зависимости от количества диапазонов, телефоны подразделяются на классы и вариацию частот в зависимости от региона использования.

Однодиапазонные — телефон может работать в одной полосе частот. В настоящее время не выпускаются, но существует возможность ручного выбора определённого диапазона частот в некоторых моделях телефонов, например Motorola C115, или с помощью инженерного меню телефона.

Двухдиапазонные (Dual Band) — для Европы, Азии, Африки, Австралии 900/1800 и 850/1900 для Америки и Канады.

Трёхдиапазонные (Tri Band) — для Европы, Азии, Африки, Австралии 900/1800/1900 и 850/1800/1900 для Америки и Канады.

Четырехдиапазонные (Quad Band) — поддерживают все диапазоны 850/900/1800/1900.

В стандарте GSM применяется GMSK-модуляция с величиной нормированной полосы BT — 0,3, где B — ширина полосы фильтра по уровню минус 3 дБ, T — длительность одного бита цифрового сообщения.

GSM на сегодняшний день является наиболее распространённым стандартом связи. По данным ассоциации GSM (GSMA) на данный стандарт приходится 82 % мирового рынка мобильной связи, 29 % населения земного шара использует глобальные технологии GSM. В GSMA в настоящее время входят операторы более чем 210 стран и территорий.

История развития

GSM сначала означало Groupe Spécial Mobile, по названию группы анализа, которая создавала стандарт. Теперь он известен как Global System for Mobile Communications (Глобальная Система для Мобильной Связи), хотя слово «Связь» не включается в сокращение. Разработка GSM началась в 1982 году группой из 26 Европейских национальных телефонных компаний. Европейская конференция почтовых и телекоммуникационных администраций (CEPT), стремилась построить единую для всех европейских стран сотовую систему диапазона 900 МГц. Достижения GSM стали «одними из наиболее убедительных демонстраций какое сотрудничество в Европейской промышленности может быть достигнуто на глобальном рынке».

В 1989 году Европейский Телекоммуникационный Институт Стандартов (ETSI) взял ответственность за дальнейшее развитие GSM. В 1990 году были опубликованы первые рекомендации. Спецификация была опубликована в 1991 году.

Коммерческие сети GSM начали действовать в Европейских странах в середине 1991 г. GSM разработан позже, чем аналоговая сотовая связь и во многих отношениях была лучше спроектирована. Северо-Американский аналог — PCS, вырастил из своих корней стандарты включая цифровые технологии TDMA и CDMA, но для CDMA потенциальное улучшение качества обслуживания так и не было никогда подтверждено.

GSM Phase 1

1982 (Groupe Spécial Mobile) — 1990 г. Global System for Mobile Communications. Первая коммерческая сеть в январе 1992 г. Цифровой стандарт, поддерживает скорость передачи данных до 9,6 кбит/с. Полностью устарел, производство оборудования под него прекращено.

В 1991 году были введены услуги стандарта GSM «ФАЗА 1».

В них входят:

Переадресация вызова (Call forwarding). Возможность перевода входящих звонков на другой телефонный номер в тех случаях, когда номер занят или абонент не отвечает; когда телефон выключен или находится вне зоны действия сети и т. п. Кроме того, возможна переадресация факсов и данных.

Запрет вызова (Call barring). Запрет на все входящие/исходящие звонки; запрет на исходящие международные звонки; запрет на входящие звонки, за исключением внутрисетевых.

Ожидание вызова (Call waiting). Эта услуга позволяет принять входящий вызов во время уже продолжающегося разговора. При этом первый абонент или по-прежнему будет находиться на связи, или разговор с ним может быть завершён.

Удержание вызова (Call Holding). Эта услуга позволяет, не разрывая связь с одним абонентом, позвонить (или ответить на входящий звонок) другому абоненту.

Глобальный роуминг (Global roaming). При посещении любой из стран, с которой ваш оператор подписал соответствующее соглашение, вы можете пользоваться своим сотовым телефоном GSM без изменения номера.

GSM Phase 2

Стандарт GSM Phase 2 принят в 1993 г.[3] Цифровой стандарт, поддерживает скорость передачи данных до 9,6 кбит/с. С 1995 г. включает диапазон 1900 МГц. Второй этап развития GSM — GSM «Фаза 2», который завершился в 1997 г., предусматривает такие услуги:

Определение номера вызывающей линии (Calling Line Identification Presentation). При входящем звонке на экране высвечивается номер вызывающего абонента.

Антиопределитель номера (Calling Line Identification Restriction). С помощью этой услуги можно запретить определение собственного номера при соединении с другим абонентом.

Групповой вызов (Multi party). Режим телеконференции или конференц-связи позволяет объединить до пяти абонентов в группу и вести переговоры между всеми членами группы одновременно.

Создание закрытой группы до десяти абонентов (Closed User Group). Позволяет создавать группу пользователей, члены которой могут связываться только между собой. Чаще всего к этой услуге прибегают компании, предоставляющие терминалы своим служащим для работы.

Информация о стоимости разговора. Сюда входят таймер, который считает время на линии, и счётчик звонков. Также благодаря этой услуге можно проверять оставшийся на счёте кредит. Возможна и другая услуга: «Совет по оплате» (Advice of Charge). По требованию пользователя происходит проверка стоимости и длительности разговора в то время, когда аппарат находится на связи.

Обслуживание дополнительной линии (Alternative Line Service). Пользователь может приобрести два номера, которые будут приписаны к одному модулю SIM. В этом случае связь выполняется по двум линиям, с предоставлением двух счетов, двух голосовых ящиков и т. п.

Короткие текстовые сообщения (Short Message Service). Возможность приёма и передачи коротких текстовых сообщений (до 160 знаков).

Система голосовых сообщений (Voice Mail). Услуга позволяет автоматически переводить входящие звонки на персональный автоответчик (голосовая почта). Пользоваться этим можно только в том случае, если у абонента активизирована услуга «переадресация вызовов».

Стандарт GSM Phase 2 считается устаревшим; но так как стандарт GSM подразумевает обратную совместимость, то старое оборудование базовых станций и телефоны могут работать (и работают) в современных сетях.

GSM Phase 2+

Следующий этап развития сетей стандарта GSM «ФАЗА 2+» не связан с конкретным годом внедрения. Новые услуги и функции стандартизируются и внедряются после подготовки и утверждения их технических описаний. Все работы по этапу «Фаза 2+» проводились Европейским институтом стандартизации электросвязи (ETSI). Количество уже внедрённых и находящихся в стадии утверждения услуг превышает 50. Среди них можно выделить следующие:

- улучшенное программное обеспечение SIM-карты;
- улучшенное полноскоростное кодирование речи EFR (Enhanced Full Rate);
- возможность взаимодействия между системами GSM и DECT;
- повышение скорости передачи данных благодаря пакетной передаче данных GPRS (General Packet RadioService) или за счёт системы передачи данных по коммутируемым каналам HSCSD (High Speed Circuit Switched Data).

Стандарты и радиоинтерфейс

Стандарты GSM создаются и публикуются Европейским институтом телекоммуникационных стандартов. Документы обозначаются GSM nn.nn, например широко известен стандарт на GSM SIM-карточки GSM 11.11.

На сегодняшний день разработано множество различных стандартов сотовой связи. Существенная часть из них уже и морально, и физически устарела, часть не нашла распространения, а другие, напротив, распространились по всему миру и нашли сотни миллионов пользователей. Вот список самых распространенных стандартов:

* AMPS
* DAMPS
* NMT-450
* GSM 900,1800,1900
* CDMA
*DECT

Наибольшее распространение, благодаря отличным функциональным возможностям (передача SMS, MMS, EMS, факсов, возможность доступа в интернет по GPRS, система GPS и т.д.), нашли полностью цифровые стандарты GSM и CDMA.

GSM-900

Цифровой стандарт мобильной связи в диапазоне частот от 890 до 915 МГц (от телефона к базовой станции) и от 935 до 960 МГц (от базовой станции к телефону). Количество реальных каналов связи гораздо больше чем написано выше в таблице, т.к присутствует еще и временное разделение каналов TDMA, т.е на одной и той же частоте могут работать несколько абонентов с разделением во времени.

В некоторых странах диапазон частот GSM-900 был расширен до 880—915 МГц (MS -> BTS) и 925—960 МГц (MS <- BTS), благодаря чему максимальное количество каналов связи увеличилось на 50. Такая модификация была названа E-GSM (extended GSM).

GSM-1800

Модификация стандарта GSM-900, цифровой стандарт мобильной связи в диапазоне частот от 1710 до 1880 МГц.

Особенности:

Максимальная излучаемая мощность мобильных телефонов стандарта GSM-1800 — 1 Вт, для сравнения у GSM-900 — 2 Вт. Большее время непрерывной работы без подзарядки аккумулятора и снижение уровня радиоизлучения.

Высокая ёмкость сети, что важно для крупных городов.

Возможность использования телефонных аппаратов, работающих в стандартах GSM-900 и GSM-1800, одновременно. Такой аппарат функционирует в сети GSM-900, но, попадая в зону GSM-1800, переключается — вручную или автоматически. Это позволяет оператору рациональнее использовать частотный ресурс, а клиентам — экономить деньги за счёт низких тарифов. В обеих сетях абонент пользуется одним номером. Но использование аппарата в двух сетях возможно только в тех случаях, когда эти сети принадлежат одной компании, или между компаниями, работающими в разных диапазонах, заключено соглашение о роуминге.

Сеть GSM 900-1800 — это единая сеть, с общей структурой, логикой и мониторингом в которой телефон никуда не переключается. Вручную можно только запретить использовать один из диапазонов в тестовых или очень старых аппаратах.

Проблема состоит в том, что зона охвата для каждой базовой станции значительно меньше, чем в стандартах GSM-900, AMPS/DAMPS-800, NMT-450. Необходимо большее число базовых станций. Чем выше частота излучения, тем хуже проникающая способность радиоволн в городской застройке.

Дальность связи в GSM лимитирована задержкой сигнала Timing advance и составляет до 35 км. При использовании режима extended cell возрастает до 75 км. Практически достижимо только в море, пустыне и горах.

CDMA

Тип стандарта: цифровой

Полоса частот: 1,23 МГц

Статус: Активно эксплуатируется

Краткое описание: Технология CDMA (система множественного доступа с кодовым разделением) изначально разработана для военных целей США, но, благодаря отличным показателям, нашла после модернизации широкое применение и в гражданской связи.

Особенности:

* Сигнал каждого абонента модулируется псевдослучайным, уникальным кодом (шумоподобным сигналом, отправляемым клиенту в начале разговора). Несущая частота сигнала меняется, согласно этому случайному правилу, в результате чего узкополосный информационный сигнал каждого пользователям расширяется во всю ширину частотного спектра (1,23 МГц в случае CDMA). В приемнике сигнал демодулируется с помощью идентичного кода, в результате чего восстанавливается изначальный сигнал. Но в то же время сигналы остальных пользователей для данного приемника продолжают оставаться расширенными и воспринимаются им лишь как шум, незначительно мешающий нормальной работе приемника.

* Отличные показатели шумоустойчивости, как следствие - снижение стоимости развертывания CDMA-сетей.

* Высокое качество передачи речи при низких показателях излучаемой мощности.

* Большая, по сравнению с GSM, емкость сети.

* Высокое качество связи в зданиях.

NMT-450

Тип стандарта: аналоговый

Частотный диапазон: 453-468 МГц

Статус: устарел и морально, и физически

Краткое описание: NMT-450 (Nordic Mobile Telephone) разработан скандинавскими учеными. Первые сотовые сети в России строились именно на базе этого стандарта - федеральная сеть "СОТЕЛ" работала именно на NMT.

Особенности:

* Большая площадь покрытия одним ретранслятором, а значит, меньшие затраты на организацию сети.

* Малое затухание сигнала на открытом пространстве, что для России с ее плотностью заселения - огромный плюс.

* Сигнал ретранслятора может добивать на 100 километров!

* Благодаря тому, что стандарт - аналоговый, обеспечивается более высокое качество передачи речи - отсутствует грубая дискретизация голосовых отсчетов.

* Плохая помехоустойчивость из-за используемых частот. Уровень индустриальных помех в этом диапазоне значительно выше, чем, скажем, на 800, 900 и 1800 МГц.

* Отсутствие секретности разговоров - их можно слушать УКВ-приемником.

* Низкая емкость сетей, что не позволяет массово использовать стандарт в крупных городах.

* Список дополнительных услуг издевательски пуст.

* NMT-трубки весят в несколько раз больше своих цифровых собратьев и крайне расточительны в плане электроэнергии и здоровья владельца.

AMPS

Тип стандарта: аналоговый

Частотный диапазон: 825-890 МГц

Статус: устарел и морально, и физически

Краткое описание: В конце восьмидесятых американские специалисты разработали специально для своей страны стандарт AMPS (Advanced Mobile Phone Service - усовершенствованная мобильная телефонная система). Завоевав популярность в других странах, в 1993 стандарт пришел в Россию. Такие сети по сей день эксплуатируются в 55 регионах, часть из них работает в аналоговом стандарте AMPS, часть - в усовершенствованном цифровом D-AMPS.

Особенности:

* Более высокая, чем у NMT-450, емкость сетей.

* Низкий уровень индустриальных и атмосферных помех благодаря используемому частотному диапазону.

* Более надежная, чем у NMT-450, связь в помещениях.

* Меньшая зона устойчивой связи для одной базовой станции, что вынуждает операторов ставить их ближе друг к другу - большие затраты.

* Почти не распространен в Европе и Азии.

AMPS уже давным-давно морально устарел, и в 1990 г. в США был разработан D-AMPS.

D-AMPS

Тип стандарта: цифровой

Частотный диапазон: 825-890 МГц

Статус: устарел морально

Краткое описание: Когда AMPS морально устарел - а это произошло довольно быстро, в 1990 году - в Штатах был разработан D-AMPS.

Особенности:

* Емкость сетей на несколько порядков выше, чем у NMT-450 и AMPS.

* Возможность эксплуатации мобильных аппаратов как в цифровом, так и в аналоговом режимах.

* Расширенный спектр дополнительных услуг.

* Емкость DAMPS-сетей ниже, чем в полностью цифровых системах, но выше, чем в аналоговых.

GPRS

Главным недостатком стандарта GSM на сегодня является низкая скорость передачи данных - максимум 9,6 Кбит/с, да и сам процесс реализован довольно убого - под данные выделяется один голосовой канал; оплата услуги, соответственно, осуществляется исходя из времени соединения, причем по тарифам, весьма схожим с речевыми. Для решения этой проблемы и был разработан стандарт передачи данных GPRS (General Packet Radio Service - услуга пакетной передачи данных по радиоканалу).

Новая система предложила пользователям мобильной связи уже совсем другие условия - максимальная скорость соединения составляет 171,2 Кбит/с, а оплата осуществляется исходя из количества реально переданной информации, трафика.

В GSM-сетях, оборудованных GPRS-модулями, более рационально распределяется радиочастотный ресурс. Не вдаваясь в сложные технические детали, можно сказать, что выигрыш в скорости достигается за счет одновременного использования для передачи данных нескольких свободных в настоящий момент каналов. Тут следует отметить, что скорость передачи информации определяется не столько теоретическими возможностями сетевого и абонентского оборудования, сколько загрузкой сети - так, из собственного опыта могу сказать, что скорость соединения в России в ближайшие несколько лет у тебя не превысит 5-6 Кбит/с.

Благодаря тому, что пакеты данных имеют значительно меньший приоритет, по сравнению с голосовой информацией, внедрение систем GPRS не приводит к ухудшению качества услуг передачи речи.

Система GPRS состоит из двух основных модулей: SGSN (Serving GPRS Support Node - узел поддержки GPRS) и GGSN (Gateway GPRS Support Node - шлюзовой узел GPRS). В некотором смысле SGSN можно назвать аналогом коммутатора сети GSM. SGSN обеспечивает доставку пакетов информации пользователям, взаимодействует с реестром абонентов, проверяет, разрешены ли запрашиваемые услуги, ведет мониторинг пользователей, организует регистрацию вновь прибывших абонентов и т.п.

Назначение GGSN легко понять из расшифровки названия - это шлюз между сотовой сетью (вернее, SGSN) и внешними информационными сетями (интернетом, провайдерскими Intranet-сетями и т.д.).

Основной задачей GGSN, таким образом, является маршрутизация (обычно совмещенная с NAT'ом) пакетов, генерируемых абонентом через SGSN. Вторичными функциями GGSN являются: динамическая выдача IP-адресов (а-ля DHCP-сервер :)), отслеживание информации о внешних сетях, подсчет трафика, тарификация и т.д.

Благодаря хорошей масштабируемости системы GPRS, оператор может увеличивать число SGSN и GGSN по мере роста числа пользователей и их суммарного трафика.

Как известно, для работы с GPRS необходимо иметь специальный телефон, поддерживающий эту технологию.

Основная характеристика такого телефона - так называемый класс GPRS. Это максимальное количество каналов, которое может задействовать аппарат для передачи данных - напомню, что один канал обеспечивает передачу данных со скоростью до 13,4 Кбит/с.

Самым первым производителем телефонов с GPRS стала французская фирма Sagem - на проходящей в Женеве выставке Telecom'99 она представила телефон Sagem MC-850, имеющий 3 канала на прием и 1 на передачу данных.

Современные телефоны способны использовать десять и более каналов для передачи данных, что, теоретически, обеспечивает отличную скорость соединения - до 20 килобайт в секунду.

В стандарте GSM определены 4 диапазона работы (ещё есть пятый):

900/1800 МГц (используется в Европе, Азии)

Характеристики	GSM-900	GSM-1800
Частоты передачи MS и приёма BTS (uplink), МГц	890 — 915	1710 — 1785
Частоты приёма MS и передачи BTS (downlink), МГц	935 — 960	1805 — 1880
Дуплексный разнос частот приёма и передачи, МГц	45	95
Количество частотных каналов связи с шириной 1 канала связи в 200 кГц	124	374
Ширина полосы канала связи, кГц	200	200

850/1900 МГц (используется в США, Канаде, отдельных странах Латинской Америки и Африки)

Характеристики	GSM-850	GSM-1900
Частоты передачи MS и приёма BTS, МГц	824 — 849	1850 — 1910
Частоты приёма MS и передачи BTS, МГц	869 — 894	1930 — 1990
Дуплексный разнос частот приёма и передачи, МГц	45	80

Структура GSM

Система GSM состоит из трёх основных подсистем:

подсистема базовых станций (BSS — Base Station Subsystem),

подсистема коммутации (NSS — Network Switching Subsystem),

центр технического обслуживания (OMC — Operation and Maintenance Centre).

В отдельный класс оборудования GSM выделены терминальные устройства — подвижные станции (MS — Mobile Station), также известные как мобильные (сотовые) телефоны.

Подсистема базовых станций

Рис.7.1. Антенны трех базовых станций на мачте

BSS состоит из собственно базовых станций (BTS — Base Transceiver Station) и контроллеров базовых станций (BSC — Base Station Controller). Область, накрываемая сетью GSM, разбита на условные шестиугольники, называемые сотами или ячейками. Диаметр каждой шестиугольной ячейки может быть разным — от 400 м до 50 км. Максимальный теоретический радиус ячейки составляет 120 км, что обусловлено ограниченной возможностью системы синхронизации к компенсации времени задержки сигнала. Каждая

ячейка покрывается находящейся в её центре одной базовой станцией, при этом ячейки частично перекрывают друг друга, тем самым сохраняется возможность передачи обслуживания без разрыва соединения при перемещении абонента из одной соты в другую. Естественно, что на самом деле сигнал от каждой станции распространяется, покрывая площадь в виде круга, а не шестиугольника, последний же является лишь упрощением представления зоны покрытия. Каждая базовая станция имеет шесть соседних в связи с тем, что в задачи планирования размещения станций входила минимизация стоимости системы. Меньшее количество соседних базовых станций приводило бы к большему перехлёсту зон покрытия с целью избегания "мёртвых зон", что в свою очередь потребовало бы более плотного расположения базовых станций. Большее количество соседних базовых станций приводило бы к излишним расходам на дополнительные станции, в то время как выигрыш от уменьшения зон перехлёста был бы уже весьма незначительным.

Базовая станция (BTS) обеспечивает приём/передачу сигнала между MS и контроллером базовых станций. BTS является автономной и строится по модульному принципу. Направленные антенны базовых станций могут располагаться на вышках, крышах зданий и т. д.

Контроллер базовых станций (BSC) контролирует соединения между BTS и подсистемой коммутации. В его полномочия также входит управление очерёдностью соединений, скоростью передачи данных, распределение радиоканалов, сбор статистики, контроль различных радиоизмерений, назначение и управление процедурой Handover.

Подсистема коммутации

NSS состоит из нижеследующих компонентов.

Центр коммутации (MSC — Mobile Switching Center)

MSC контролирует определённую географическую зону с расположенными на ней BTS и BSC. Осуществляет установку соединения к абоненту и от него внутри сети GSM, обеспечивает интерфейс между GSM и ТфОП, другими сетями радиосвязи, сетями передачи данных. Также выполняет функции маршрутизации вызовов, управление вызовами, эстафетной передачи обслуживания при перемещении MS из одной ячейки в другую. После завершения вызова MSC обрабатывает данные по нему и передаёт их в центр расчётов для формирования счета за предоставленные услуги, собирает статистические данные. MSC также постоянно следит за положением MS, используя данные из HLR и VLR, что необходимо для быстрого нахождения и установления соединения с MS в случае её вызова.

Домашний регистр местоположения (HLR — Home Location Registry)

Содержит базу данных абонентов, приписанных к нему. Здесь содержится информация о предоставляемых данному абоненту услугах, информация о состоянии каждого абонента,

необходимая в случае его вызова, а также Международный Идентификатор Мобильного Абонента (IMSI — International Mobile Subscriber Identity), который используется для аутентификации абонента (при помощи AUC). Каждый абонент приписан к одному HLR. К данным HLR имеют доступ все MSC и VLR в данной GSM-сети, а в случае межсетевого роуминга — и MSC других сетей.

Гостевой регистр местоположения (VLR — Visitor Location Registry)

VLR обеспечивает мониторинг передвижения MS из одной зоны в другую и содержит базу данных о перемещающихся абонентах, находящихся в данный момент в этой зоне, в том числе абонентах других систем GSM — так называемых роумерах. Данные об абоненте удаляются из VLR в том случае, если абонент переместился в другую зону. Такая схема позволяет сократить количество запросов на HLR данного абонента и, следовательно, время обслуживания вызова.

Регистр идентификации оборудования (EIR — Equipment Identification Registry)

Содержит базу данных, необходимую для установления подлинности MS по IMEI (International Mobile Equipment Identity). Формирует три списка: белый (допущен к использованию), серый (некоторые проблемы с идентификацией MS) и чёрный (MS, запрещённые к применению). У российских операторов (и большей части операторов стран СНГ) используются только белые списки, что не позволяет раз и навсегда решить проблему кражи мобильных телефонов.

Центр аутентификации (AUC — Authentification Center)

Здесь производится аутентификация абонента, а точнее — SIM (Subscriber Identity Module). Доступ к сети разрешается только после прохождения SIM процедуры проверки подлинности, в процессе которой с AUC на MS приходит случайное число RAND, после чего на AUC и MS параллельно происходит шифрование числа RAND ключом Ki для данной SIM при помощи специального алгоритма. Затем с MS и AUC на MSC возвращаются «подписанные отклики» — SRES (Signed Response), являющиеся результатом данного шифрования. На MSC отклики сравниваются, и в случае их совпадения аутентификация считается успешной.

Подсистема OMC (Operations and Maintenance Center)

Соединена с остальными компонентами сети и обеспечивает контроль качества работы и управление всей сетью. Обрабатывает аварийные сигналы, при которых требуется вмешательство персонала. Обеспечивает проверку состояния сети, возможность прохождения вызова. Производит обновление программного обеспечения на всех элементах сети и ряд других функций.

Преимущества и недостатки

Преимущества стандарта GSM:

Меньшие по сравнению с аналоговыми стандартами (NMT-450, AMPS-800) размеры и вес телефонных аппаратов при большем времени работы без подзарядки аккумулятора. Это достигается в основном за счёт аппаратуры базовой станции, которая постоянно анализирует уровень сигнала, принимаемого от аппарата абонента. В тех случаях, когда он выше требуемого, на сотовый телефон автоматически подаётся команда снизить излучаемую мощность.

Хорошее качество связи при достаточной плотности размещения базовых станций.

Большая ёмкость сети, возможность большого числа одновременных соединений.

Низкий уровень индустриальных помех в данных частотных диапазонах.

Улучшенная (по сравнению с аналоговыми системами) защита от подслушивания и нелегального использования, что достигается путём применения алгоритмов шифрования с разделяемым ключом.

Эффективное кодирование (сжатие) речи. EFR-технология была разработана фирмой Nokia и впоследствии стала промышленным стандартом кодирования/декодирования для технологии GSM (см. GSM-FR, GSM-HR и GSM-EFR)

Широкое распространение, особенно в Европе, большой выбор оборудования.

Возможность роуминга. Это означает, что абонент одной из сетей GSM может пользоваться сотовым телефонным номером не только у себя «дома», но и перемещаться по всему миру переходя из одной сети в другую не расставаясь со своим абонентским номером. Процесс перехода из сети в сеть происходит автоматически, и пользователю телефона GSM нет необходимости заранее уведомлять оператора (в сетях некоторых операторов, могут действовать ограничения на предоставление роуминга своим абонентам, более детальную информацию можно получить обратившись непосредственно к своему GSM оператору)

Недостатки стандарта GSM

Искажение речи при цифровой обработке и передаче.

Связь возможна на расстоянии не более 120 км от ближайшей базовой станции даже при использовании усилителей и направленных антенн. Поэтому для покрытия определённой площади необходимо большее количество передатчиков, чем в NMT-450 и AMPS.

Моделирование канала стандарта GSM в MATLAB Simulink

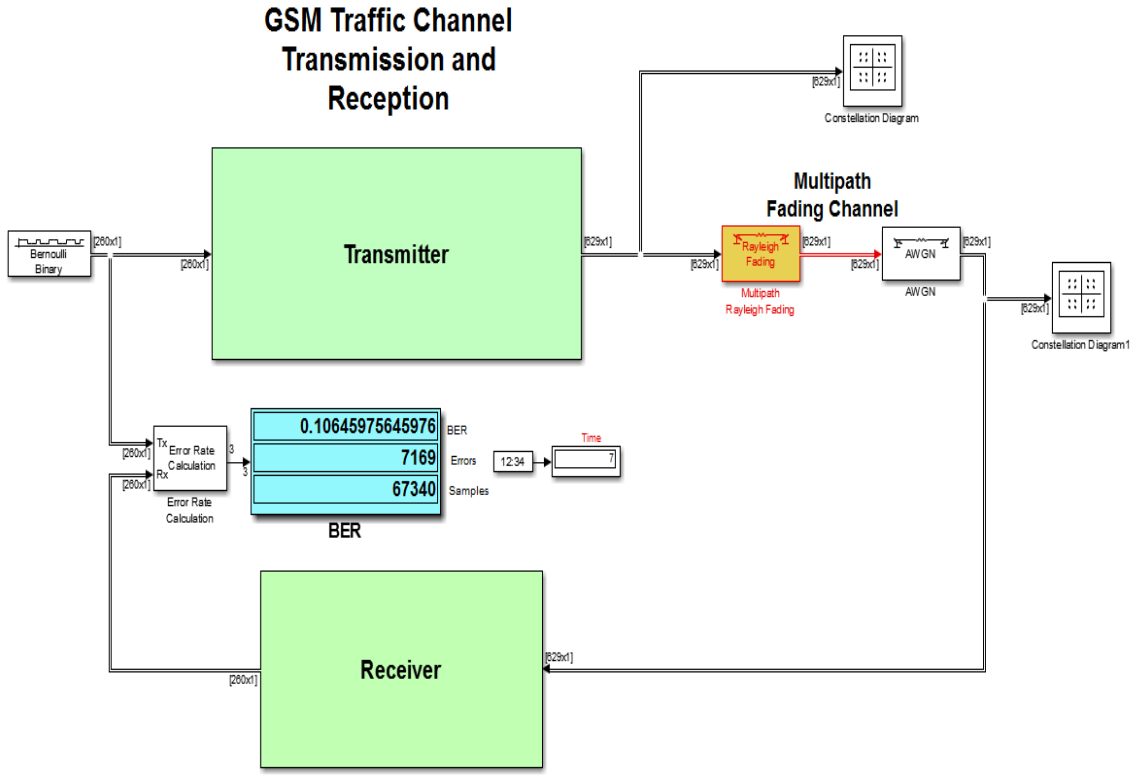


Рис. 7.2. Модель GSM в Simulink MATLAB 2015

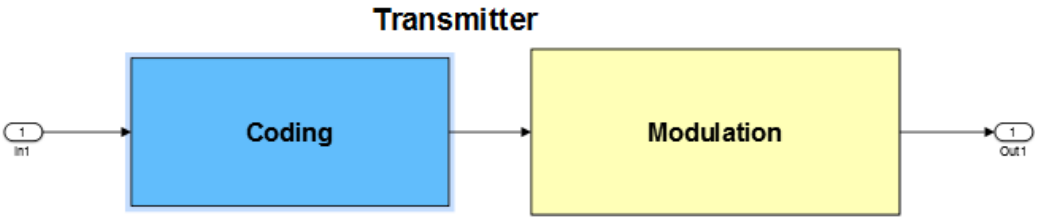


Рис. 7.3. Схема передатчика

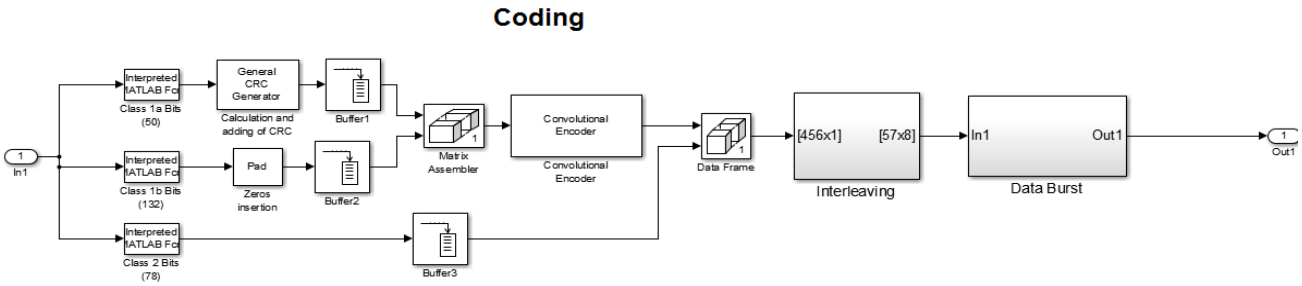


Рис. 7.4. Схема кодера

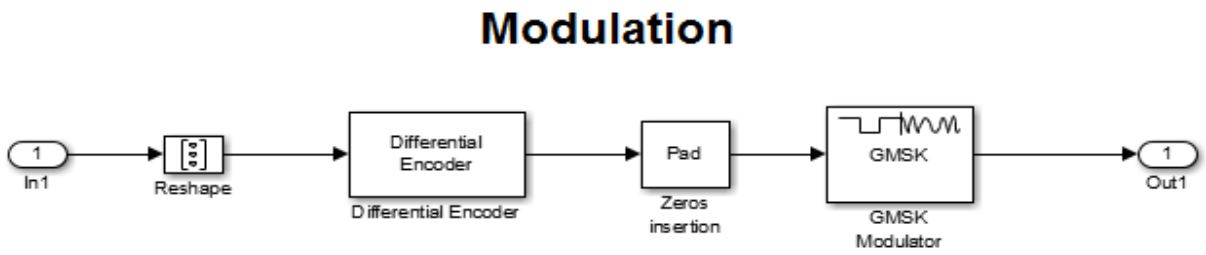


Рис. 7.5. Схема модулятора

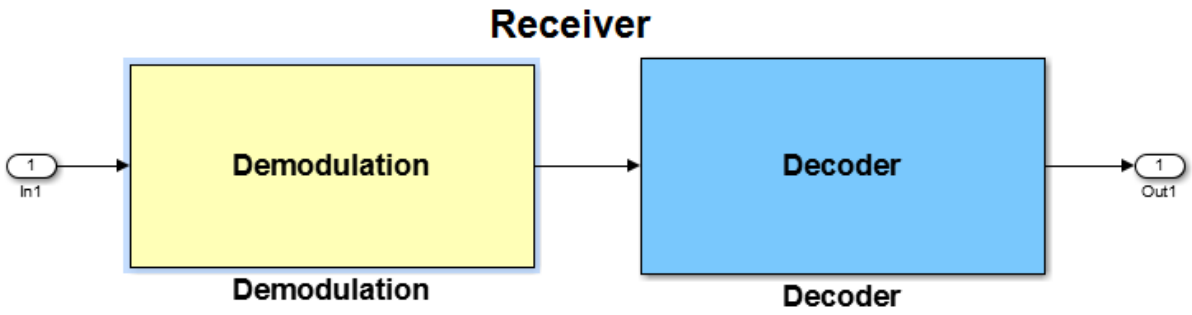


Рис. 7.6. Схема приемника

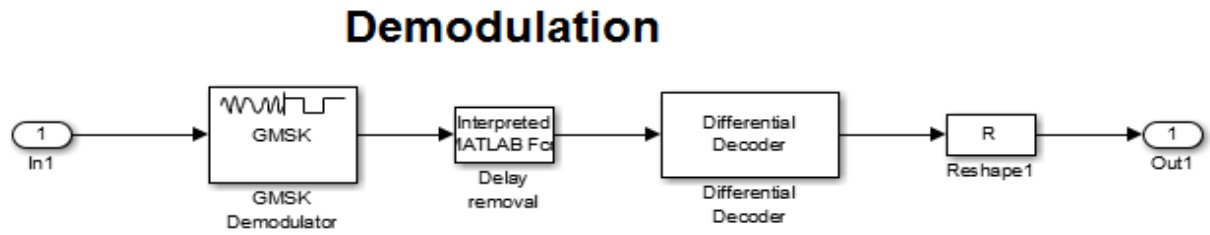


Рис. 7.7. Схема демодулятора

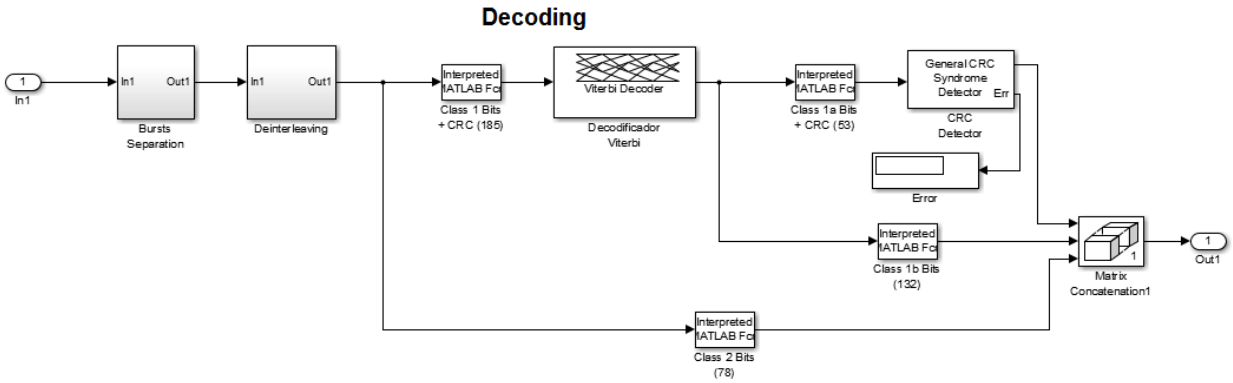


Рис. 7.8. Схема декодера

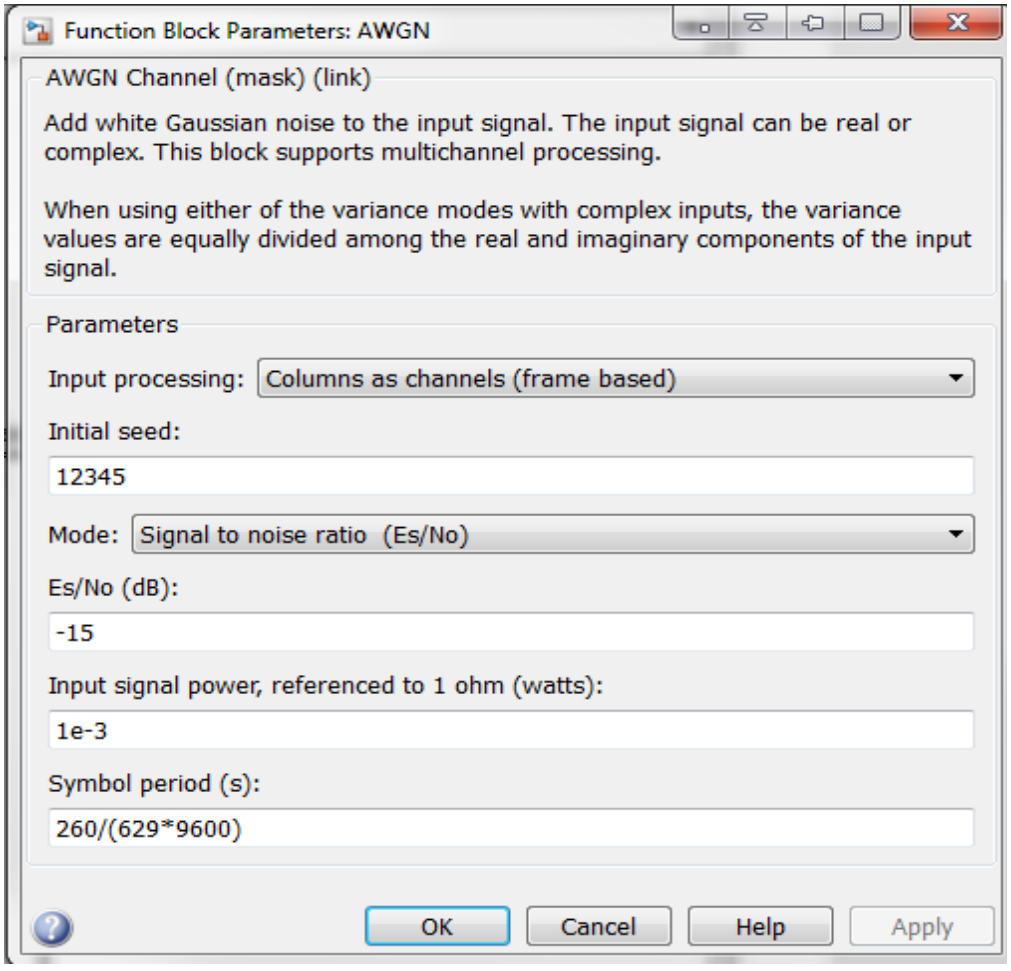


Рис. 7.9. Изменение отношения сигнал/шум.

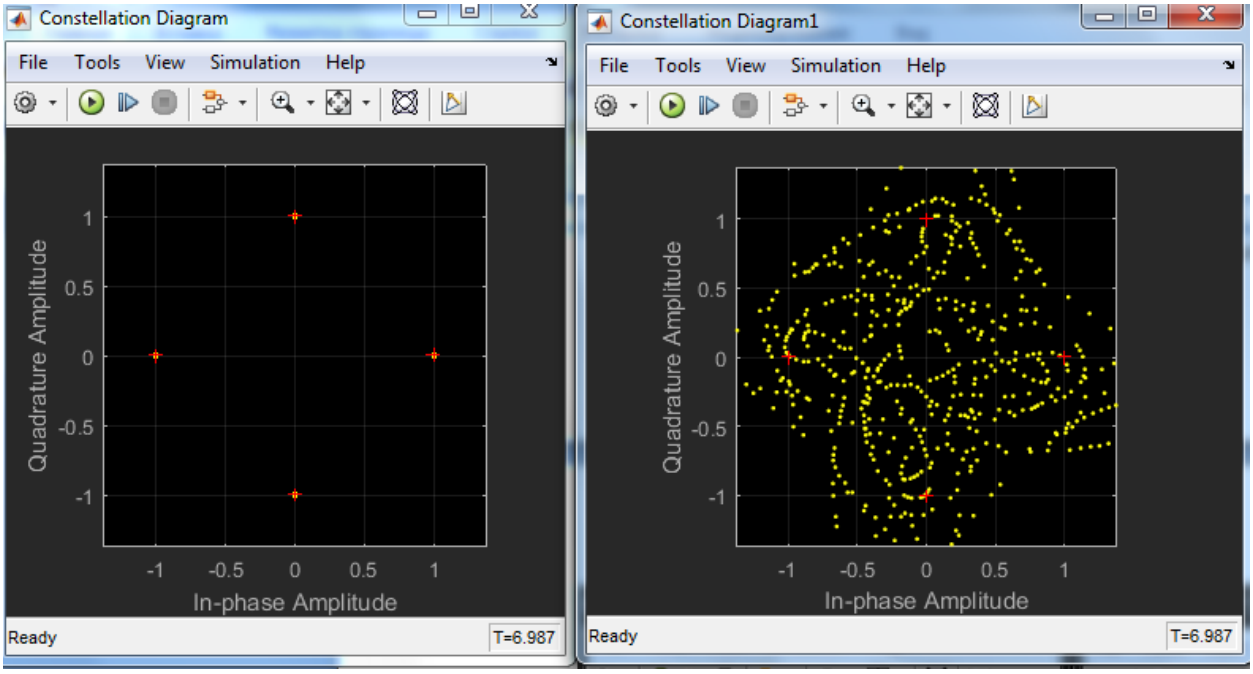


Рис. 7.10. Сравнение передаваеваемого созвездия и принятого, при отношении С/Ш – 20 Дб.

BER

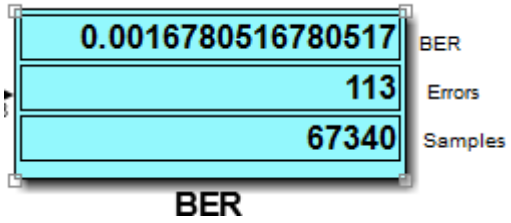


Рис. 7.11. BER при отношении С/Ш 15 Дб.

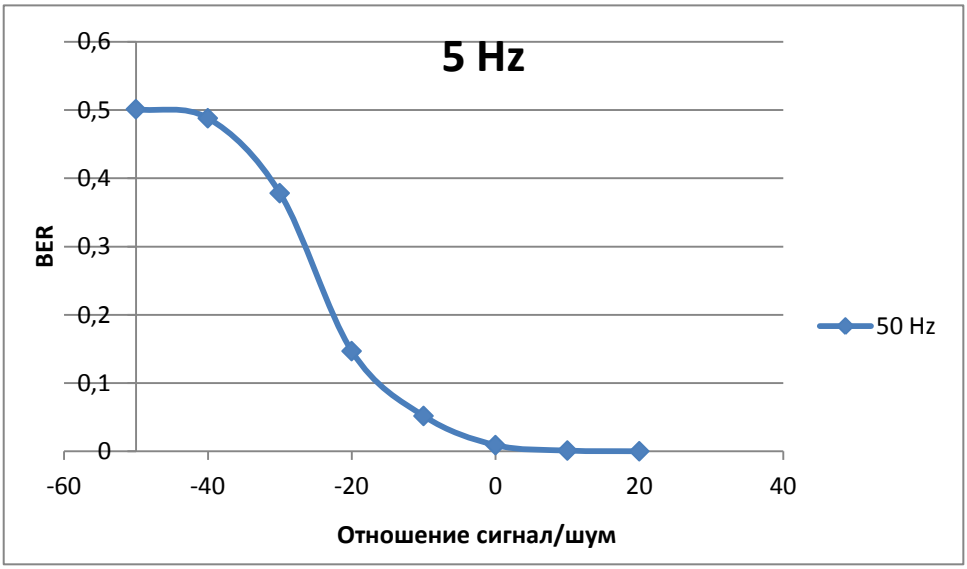


Рис. 7.12. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 5 Гц

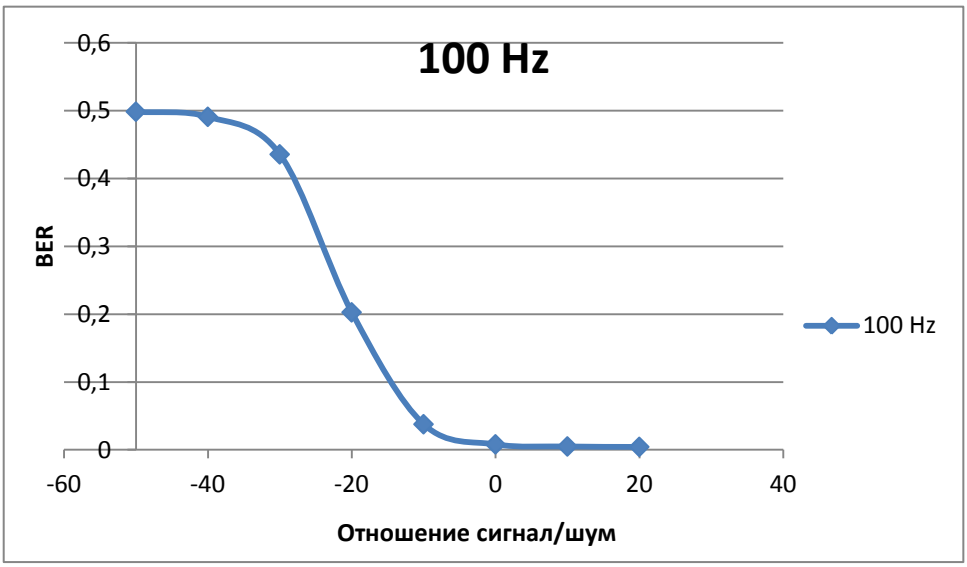


Рис. 7.13. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 100 Гц

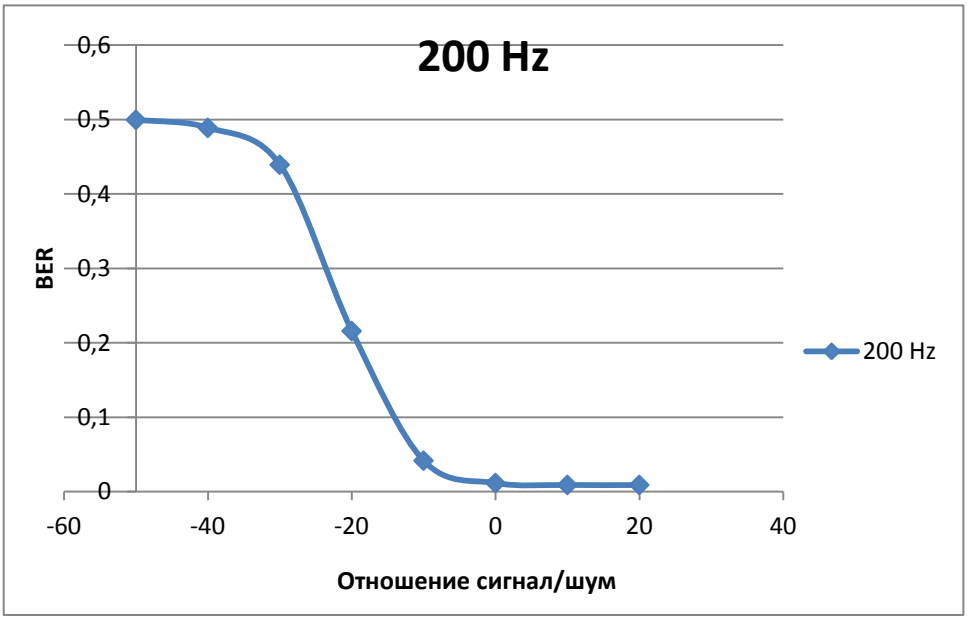


Рис. 7.14. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 200 Гц

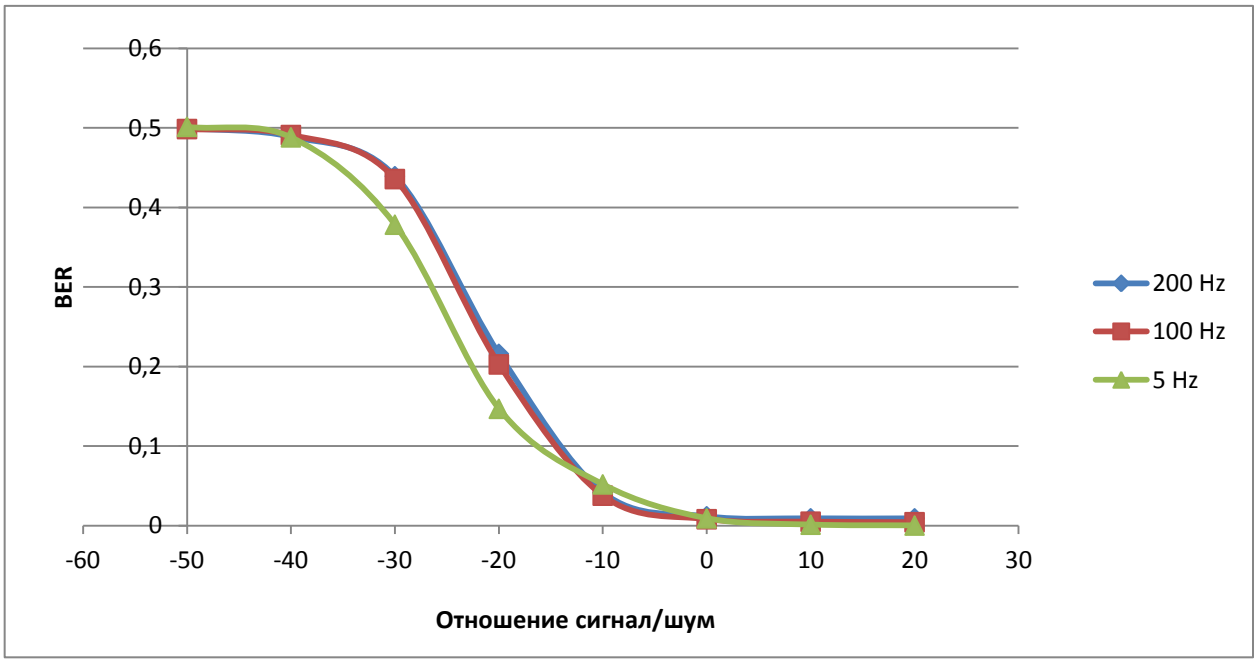


Рис. 7.15. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 5, 100, 200 Гц

В ходе данной работы мы исследовали стандарт GSM. Он позволяет производить эффективную передачу сигнала при довольном малом соотношении Сигнал Шум. Сигнал GSM зависим от Доплеровского эффекта, но учитывая, что скорость ЭМ волн крайне большая, по сравнению со скоростью обьектов связи, то этот эффект нормализуется.

7.2. Системы мобильной связи стандарта CDMA

В настоящее время развиваются системы мобильной связи, так как каждый год осуществляется рост числа абонентов, что приводит к загруженности сети, необходимости улучшения качества связи, улучшения емкости базовых станций, а также увеличения зоны покрытия сот. Но необходимо улучшать и безопасность мобильной связи, так как злоумышленники могут осуществить перехват информационного сигнала.

Новые поколения сотовой связи появляются достаточно быстро, но их внедрение требует значительных временных ресурсов, поэтому до сих пор основополагающими считаются технологии CDMA и GSM, но технология CDMA работает не только как отдельный стандарт, эта технология используется, например, в LTE.

CDMA - система множественного доступа с кодовым разделением - стала, возможно, самой многообещающей системой, появившейся на мировом рынке. Десятилетия назад эта технология использовалась в военной связи (США), а сегодня известна всем как глобальный цифровой стандарт для коммерческих систем коммуникаций. Технология использования CDMA была протестирована, стандартизирована, лицензирована и запущена в производство большинством поставщиков беспроводного оборудования и применяется во всем мире. В отличие от других методов доступа абонентов к сети, где энергия сигнала концентрируется на выбранных частотах или временных интервалах, сигналы CDMA распределены в непрерывном частотно-временном пространстве. Фактически метод манипулирует и частотой, и временем, и энергией.

CDMA применяется в 32 странах Азии и Океании, 2 странах Северной Америки, 14 странах Европы и 45 странах Африки.

История технологии CDMA берёт своё начало в 30-е годы прошлого (XX) столетия. В 1935 году в СССР академик Агеев Дмитрий Васильевич издал небольшим тиражом брошюру под странным названием "Кодовое разделение каналов". В ней были определены основы ортогонального разделения сигналов, разделения сигналов по форме. В то время реально существовал только один способ разделения каналов связи – частотный. И относилось это, в основном, к каналам радиосвязи. При таком методе каждый канал занимает некоторую свою полосу в общем спектре частот. Эти полосы относительно узки и разделены между собой защитными интервалами. Частотный диапазон ещё не был так перегружен как сегодня, поэтому использование такого способа разделения каналов связи считалось достаточно простым и логичным, поскольку осуществлялась манипуляция только одним параметром сигнала – частотой. Однако учёные, работавшие в области разработок новейших систем связи, в общем, и радиосвязи, в частности, понимали, что такая идиллия не будет долгой.

Кроме того, узкополосные радиосигналы очень чувствительны к селективным замираниям. Требовалось разработать методику, минимизирующую потери полезного сигнала за счёт селективных замираний и позволяющую бережнее относится к используемому диапазону частот.

Несколько позже, примерно в одно и то же время, появляются работы «Математическая теория связи» Клода Шеннона (США) и «Теория потенциальной помехоустойчивости» Владимира Александровича Котельникова (СССР).

Впервые радиооборудование, использующее кодовое разделение каналов, появилось в США где-то в конце 50-х годов. Технология CDMA нашла применение в военных системах, где успешно отработала более двух десятков лет. Во второй половине 80-х годов военное ведомство США рассекретило данную технологию и разрешило ее использование в гражданских средствах радиосвязи (диапазон 800 МГц).

В сентябре 1995 года в Гонконге фирма HUTCHISON начала развертывание первой в мире коммерческой сети CDMA, используя базовое оборудование Motorola (базовые станции SC 9600 и коммутирующее оборудование EMX 2500) и мобильные телефоны Qualcomm. На конец 1996 года эта сеть насчитывала 113 сот, работала на одном частотном канале с полосой 1,25 МГц и обслуживала более 40.000 абонентов. Правда, соты CDMA были наложены на существующую сеть AMPS и мобильные терминалы работали в дуалмодовом режиме, т.е. при сбое в CDMA-сети абонентский терминал автоматически переключался в сеть AMPS (FDMA). В Корее в январе 1996 года фирма KMT, используя оборудование Gold Star, начала коммерческую эксплуатацию CDMA-сети. А в апреле Shinsengi Telecom начала создавать новую сеть на базе оборудования Samsung, Sony, Qualcomm. На конец 1996 года эти сети обслуживали более 200.000 клиентов. Корея приняла IS-95 в качестве национального стандарта сотовой связи. В США развертыванием CDMA-сетей занимаются такие фирмы, как Air Touch (Сан-Диего, Лос-Анджелес), BANM (Трентон, Нью-Джерси), 360-Communications (Лас-Вегас, Невада). Они используют базовое оборудование Qualcomm, Lucent Technologies, Motorola, а также абонентские терминалы фирм Qualcomm, Sony, Nortel. В Австралии, в канун Олимпийских игр, были построены сети сотовой мобильной радиотелефонной связи в Сиднее и Мельбурне на базе оборудования CDMA-one (IS-95) производства фирмы Samsung.

Кроме вышеназванного стандарта (IS-95) в 1999 году был разработан и широкополосный вариант - W-CDMA (Ericsson, Швеция), функционирующий в диапазоне 1800 МГц. Он предназначался для использования в районах с высокой плотностью населения, так как обладал ещё большей пропускной способностью.

Стандарты CDMA

В CDMA системах каждый голосовой поток отмечен своим уникальным кодом и передается на одном канале одновременно со многими другими кодированными голосовыми потоками. Принимающая сторона использует тот же код для выделения сигнала из шума. Единственное отличие между множественными голосовыми потоками это уникальный код. Канал, как правило, очень широк и каждый голосовой поток занимает целиком всю ширину диапазона. Эта система использует наборы каналов шириной 1.23МГц. Голос кодируется на скорости 8.55кбит/с, но определение голосовой активности и различные скорости кодирования могут урезать поток данных до 1200бит/с. В системах CDMA могут устанавливаться очень прочные и защищенные соединения, несмотря на экстремально низкую величину мощности сигнала, теоретически - сигнал может быть слабее, чем уровень шума

Стандарт CDMAOne

Стандарт cdmaOne, существует в вариациях IS-95a, IS-95b (cellular по американской терминологии, 800 МГц) и J-STD-008 (PCS, диапазон 1900). Аббревиатура IS (interim standard - временной стандарт) используется для учета в Ассоциации телекоммуникационной промышленности TIA (Telecommunications Industry Association). Как правило, в сетях cdmaOne используется IS-95a, он обеспечивают передачу сигнала со скоростью 9,6 кбит/с (с кодированием) и 14,4 кбит/с (без кодирования). Версия IS-95b основана на объединении нескольких каналов CDMA, организуемых в прямом направлении (от базовой станции к мобильной). Скорость может увеличиваться до 28,8 кбит/с (при объединении двух каналов по 14,4 кбит/с) или до 115,2 кбит/с (8 каналов по 14,4 кбит/с). Собственно, кроме IS-95 сети cdmaOne используют еще целый набор протоколов и стандартов, их список можно найти в любой достаточно глубокой статье по этой теме. Прямой и обратный каналы располагаются соответственно в диапазонах 869,040-893,970 и 824,040-848,860 МГц. Используются 64 кода Уолша и несущие в 1.25 МГц.

Стандарт WCDMA

WCDMA (Wideband Code Division Multiple Access - широкополосный CDMA) - технология радиоинтерфейса избранная большинством операторов сотовой связи Японии и (в январе 1988 года) институтом ETSI (European Telecommunications Standards Institute) для обеспечения широкополосного радиодоступа с целью поддержки услуг третьего поколения.

Технология оптимизирована для предоставления высокоскоростных мультимедийных услуг типа видео, доступа в Интернет и видеоконференций; обеспечивает скорости доступа вплоть до 2 Мбит/с на коротких расстояниях и 384 Кбит/с на больших с полной мобильностью. Такие величины скорости передачи данных требуют широкую полосу частот,

посему ширина полосы WCDMA составляет5 Мгц. Технология может быть добавлена к существующим сетям GSM и PDC, что делает стандарт WCDMA наиболее перспективным с точки зрения использования сетевых ресурсов и глобальной совместимости.

WCDMA (широкополосный множественный доступ с кодовым разделением каналов) представляет собой технологию, использующую расширенную полосу пропускания и разновидность принципа DMA. Это технология мобильной радиосвязи третьего поколения, обеспечивающая значительно более высокие скорости передачи данных, чем стандарт GSM. WCDMA поддерживает передачу голоса, изображений, данных и видео в сетях мобильной связи на скорости до 2 Мбит/с (локальный доступ) или 384 кбит/с (глобальный доступ). WCDMA используется в основном в Европе при переходе от стандарта GSM к стандарту UMTS.

Стандарт CDMA2000

Стандарт cdma2000 является дальнейшим развитием стандарта 2 поколения cdmaOne. Дальнейшим развитием cdmaOne должен был стать IS-95c, и именно это обозначение очень часто используется производителями. Официальным обновлением стандарта, разработанным компанией Qualcomm и утвержденным ITU (Международный союз электросвязи, International Telecommunication Union), является cdma2000. В документах Lucent Technologies встречается обозначение IS-2000. Наконец, международный союз электросвязи (МСЭ) отобрал из десяти предложенных проектов пять радиоинтерфейсов третьего поколения IMT-2000 (International Mobile Telecommunications System - 2000 - Международная система мобильной связи - 2000), в их числе - IMT-MC (Multi Carrier), который представляет собой модификацию многочастотной системы cdma2000, в которой обеспечивается обратная совместимость с оборудованием стандарта cdmaOne (IS-95).

Еще один из пяти стандартов IMT-2000 - IMT-DS (Direct Spread) - построен на базе проектов W-CDMA и взят за основу европейской системы UMTS.

На начало 2003г. из 127 миллионов пользователей CDMA почти 15 миллионов использовали технологию cdma2000. В течение первых семи месяцев 2002 года, в Азии и Америке было запущено 11 сетей CDMA2000 и общее количество этих сетей составляло 18. Это - 99% рынка 3G, на IMT-MC приходилось 14.8 миллионов абонентов, на UMTS - 0.13 миллиона. Однако, стоит отметить, что реализованная фаза cdma2000 1X все же не является полноценным 3G, ибо не дотягивает до обязательных двух мегабит. Поэтому ее чаще называют 2.5G.

Изначально cdma2000 (IMT-MC) разделили на две фазы - 1X и 3X. Именно к первой фазе применяется название IS-95C. А вторую позже назвали 1X-EV (evolution), разделив ее на две фазы - cdma2000 1X EV-DO (data only) и cdma2000 1X EV-DV (data & voice).

И именно стандарт cdma2000 1X EV-DO подразумевается под 3G IMT-MC. Стандарт 1x-EV-DO был принят TIA в октябре 2000 года и предусматривает следующую схему функционирования: аппарат одновременно производит поиск сети 1x и 1xEV, передачу данных осуществляет с помощью 1xEV, голоса - с помощью 1x. Стандарт 1xEV-DV полностью соответствует всем требованиям 3G.

Следует отметить, что стандарты семейства cdma2000 не требуют организации отдельной полосы частот и в ходе их эволюционного развития от cdmaOne могут быть реализованы во всех частотных диапазонах, используемых системами сотовой подвижной связи (450, 700, 800, 900, 1700, 1800, 1900, 2100 МГц).

Структура и формирование сигналов

Схема кодирования в прямом канале (от базовой станции к абоненту).

Базовая скорость передачи данных в канале составляет 9,6 кбит/с, что достигается добавлением дополнительных корректирующих двоичных символов к цифровому потоку вокодера 8,55 кбит/с.

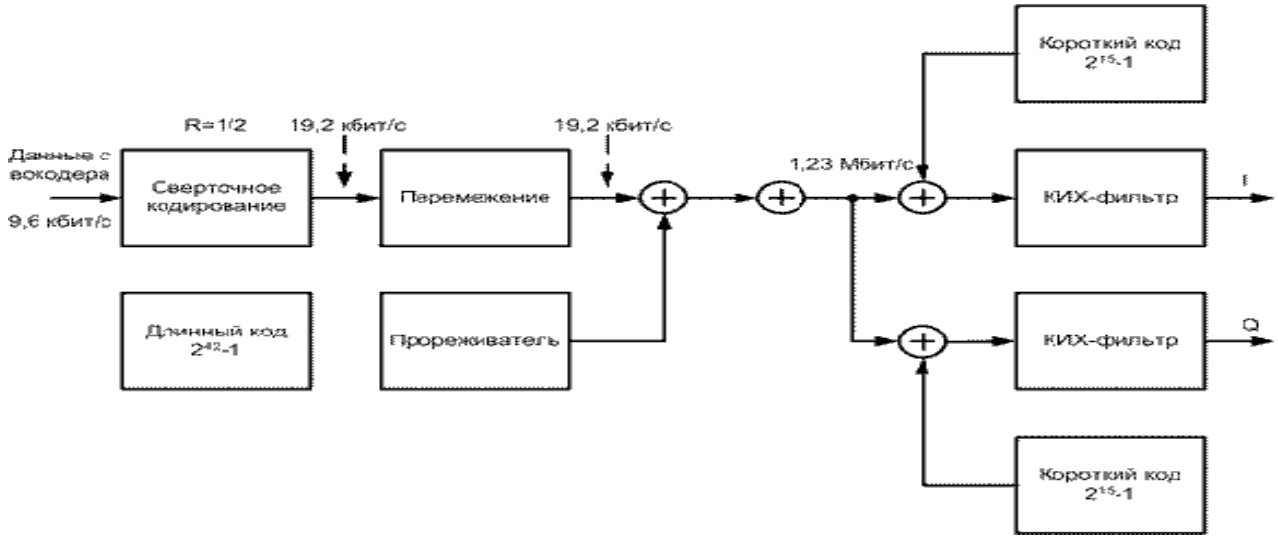


Рис. 7.16. Схема кодирования в прямом канале

Для реализации на приемной стороне прямой коррекции ошибок (без повторной передачи сообщения) в канале используется избыточное кодирование. Для этого базовый цифровой поток разбивается на пакеты длительностью по 20 мс и подается на сверточный кодер с половинной скоростью. На его выходе число битов удваивается. Затем данные перемежаются, т. е. перемешиваются во временном интервале 20 мс. Это делается для того, чтобы равномерно распределить в потоке данных (после обратного перемежения) потерянные во время передачи биты. Известно, что ошибочно принятые символы обычно формируют группы. В то же время, схема прямой коррекции ошибок работает наилучшим образом, когда ошибки распределены равномерно во времени. Это происходит после осуществления на приемной стороне процедуры, обратной перемежению при передаче.

После перемежения цифровой поток преобразуется с помощью длинного кода и логической операции "исключающее ИЛИ" (сложение по модулю два). По определению, длинными кодами (кодами максимальной длины - М-последовательностями) являются коды, которые могут быть получены с помощью регистра сдвига или элемента задержки заданной длины.

Максимальная длина двоичной последовательности, которая может быть получена с помощью генератора, построенного на основе регистра сдвига, равна 2n-1 двоичных символов, где n - число разрядов регистра сдвига. В аппаратуре стандарта CDMA длинный код формируется в результате нескольких последовательных логических операций с псевдослучайной двоичной последовательностью, генерируемой в 42-разрядном регистре сдвига, и двоичной 32-битовой маской, которая определяется индивидуально для каждого абонента. Такой регистр сдвига применяется во всех базовых станциях этого стандарта для обеспечения режима синхронизации всей сети. Длина М-последовательности при этом составляет 4 398 046 511 103 бит и если ее элементы формируются с тактовой частотой, например, 450 МГц, то период повторения будет составлять 9773,44 с= 2 ч 43 мин. Это значит, что если даже удастся засинхронизировать приемник в случае несанкционированного перехвата, то чтобы определить структуру сигнала-носителя необходимо вести наблюдение в течение почти 3-х часов, а с применением индивидуальной 32-битовой маски 'подслушивание" практически исключено. Так как информационный поток имеет скорость 19,2 Кбит/с, то в прямом канале используется только каждый 64-й символ длинного кода. Следующий этап преобразования сообщения - кодирование с помощью кодов Уолша. Любая строка матрицы Уолша ортогональна другой строке. Матрица Уолша размером 2 имеет вид:

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Матрицы больших размеров образуются следующим образом:

$$W_{2N} = \begin{pmatrix} W_N & W_N \\ W_N & -W_N \end{pmatrix}$$

т.е., например,

$$W_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Можно показать, что строки матрицы Уолша ортогональны. Ортогональность строк x и y длиной N определяется следующим условием:

$$\sum_{i=1}^{N} x_i y_i = 0$$

По сути в этом случае вычисляется значение ВКФ двух различных строк при временном сдвиге равном нулю.

Один ряд матрицы Уолша ставится в соответствие каналу связи между абонентом и базовой станцией. Если на входе кодера "0", то посылается соответствующий ряд матрицы (код Уолша), если "1" - посылается последовательность, сформированная путем логического отрицания соответствующего ряда матрицы (кода Уолша). При точном совпадении начала пришедшей последовательности и имеющейся (строка матрицы W64) наблюдаются пики корреляционной функции положительной и отрицательной полярностей - в зависимости от передаваемого бита. В случае обработки "чужого" сигнала на выходе в момент окончания сигнала не будет ничего, т.е. происходит разделение каналов при приеме абонентской станцией. Кодирование по Уолшу повышает скорость информационного потока с 19,2 Кбит/с до 1,2288 Мбит/с. Соответственно расширяется и спектр сигнала. На заключительном этапе двоичный поток разделяется между синфазным и квадратурным каналами (I- и Q-каналами) для последующей передачи с использованием квадратурной фазовой манипуляции (QPSK). До подачи на смесители цифровой поток в каждом из каналов преобразуется с помощью короткого кода и операции сложения по модулю два.

Короткий код представляет собой псевдослучайную двоичную последовательность длиной 32768 двоичных символов, генерируемую со скоростью 1,3288 Мбит/с. Эта последовательность является общей для всех базовых и подвижных станций в сети. Короткий код формируется в 15-разрядном регистре сдвига с линейной обратной связью. Результирующий двоичный поток в каждом канале проходит через цифровой фильтр с конечной импульсной характеристикой (КИХ-фильтр), что позволяет ограничить полосу

излучаемого сигнала. Частота среза фильтра составляет около 615 кГц. Полученные аналоговые сигналы поступают на соответствующие входы I/Q-модулятора. Ряд информационных сигналов образуется путем слияния I- и Q-каналов.

Поскольку все пользователи получают объединенный сигнал, то для выделения информации необходимо передавать опорный сигнал по каналу, получившему название пилотного. В пилотном канале передается нулевой информационный сигнал, код Уолша для этого канала формируется из нулевого ряда матрицы Уолша (все единицы). Другими словами, в пилотном канале передается только короткий код. Обычно на нем излучается около 20% общей мощности. Опорный сигнал необходим для последующей фазовой демодуляции. Короткий код позволяет многократно использовать в каждой ячейке один и тот же набор кодов Уолша. Каждая базовая станция имеет свой временной сдвиг при формировании кода и поэтому может быть однозначно определена в сети. Основано это на уже описанном свойстве псевдослучайных двоичных последовательностей: значение АКФ близко к нулю для всех временных смещений более одной длины бита.

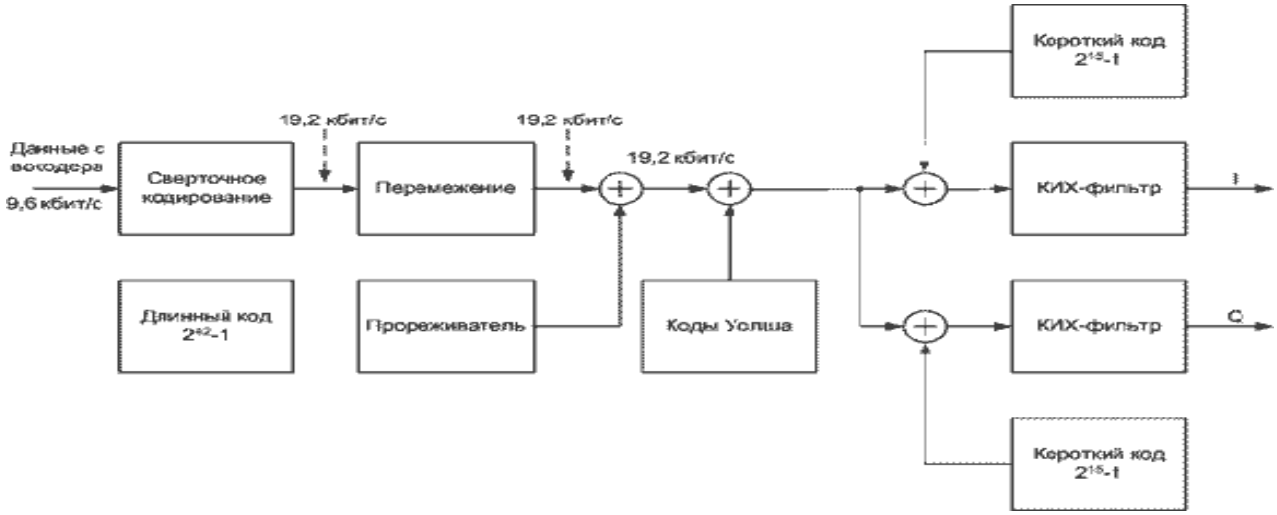


Рис. 7.17. Схема кодирования в обратном канале.

В обратном канале (от абонента к базовой станции) применяется другая схема кодирования. Подвижная станция не может использовать преимуществ трансляции опорного сигнала. В этом случае необходимо было бы передавать два сигнала, что значительно усложнило бы демодуляцию в приемнике базовой станции. В обратном канале применяется такой же, как и в прямом, вокодер и сверточное кодирование со скоростью 1/3, что повышает скорость передачи данных с базовой 9,6 до 28,8 кбит/с, и перемежение в пакете длительностью 20 мс. После перемежения выходной поток разбивается на слова по шесть битов в каждом. Шестибитовому слову можно поставить в соответствие один из 64 кодов Уолша. Таким образом, каждый абонентский терминал использует весь их набор. После этой операции скорость потока данных повышается до 307,2 Кбит/с. Далее поток преобразуется с помощью длинного кода, аналогичного используемому базовой станцией. На этом этапе

происходит разделение пользователей. Абонентская емкость системы определяется обратным каналом. Для ее увеличения применяется регулирование мощности в обратном канале, методы пространственного разнесения приема на базовой станции и др. Окончательное формирование потоков данных происходит таким же образом, как и в базовой станции, за исключением дополнительного элемента задержки на 1/2 длительности символа в Q-канале для реализации, смещенной QPSK.

В системе CDMA применяются квадратурная фазовая манипуляция (QPSK) в базовой и смещенная QPSK в подвижных станциях. При этом информация извлекается путем анализа изменения фазы сигнала, поэтому фазовая стабильность системы - критичный фактор при обеспечении минимальной вероятности появления ошибки в сообщениях. Применение смещенной QPSK позволяет снизить требования к линейности усилителя мощности подвижной станции, так как амплитуда выходного сигнала при этом виде модуляции изменяется значительно меньше. До того, как интерференционные помехи будут подавлены методами цифровой обработки сигналов, они должны пройти через высокочастотный тракт приемника и не вызвать насыщения малошумящего широкополосного усилителя (МШУ) и смесителя. Это заставляет разработчиков системы искать баланс между динамическими и шумовыми характеристиками приемника.

Рис. 7.18. Структурная схема CDMA

Моделирование CDMA2000 1xRTT

Модель состоит из трех основных блоков:

Базовая станция (передатчик);

Канал;

Мобильная станция (приемник).

Канал имеет три режима работы:

Нет канала;

Канал с шумами;

Канал с многолучевым распространением.

Мобильный приемник состоит из декодера и приемника, которые выполняют все операции необходимые декодирования сигнала.

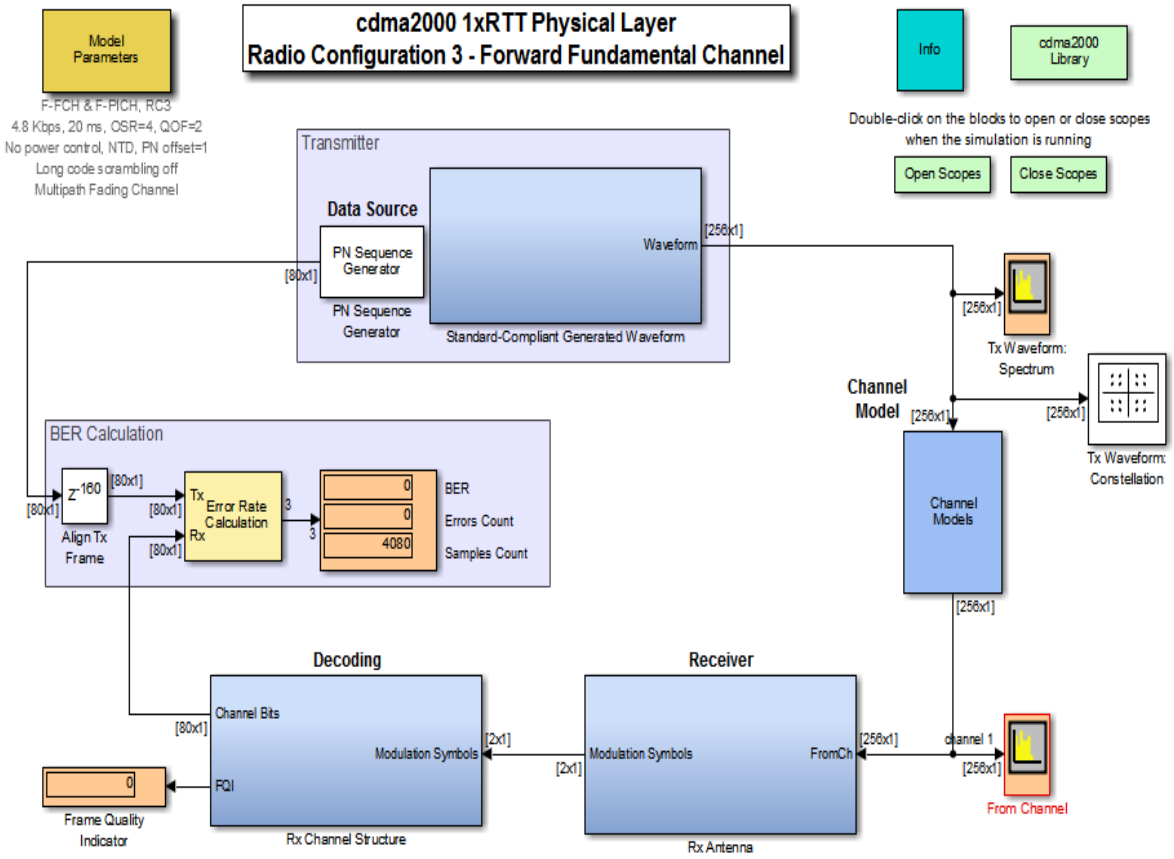


Рис.7.19. Модель CDMA2000 1xRTT в MATLAB R2015b

Развернутая модель передатчика представлена на рисунке 5.20.

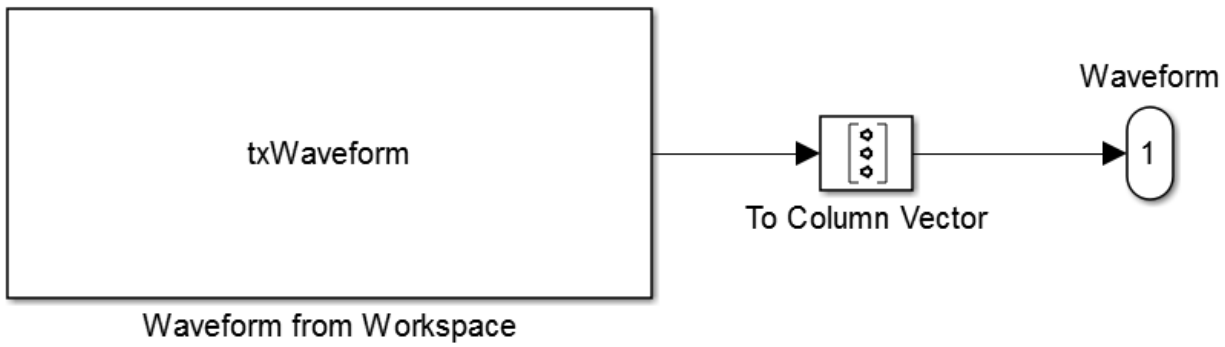


Рис. 7.20. Модель передатчика

Блок txWaveform содержит в себе длинный программный код посредством которого и генерируется сигнал, далее этот сигнал формируется в вектор с помощью блока To Column Vector. Этот вектор передается по каналу и затем поступает в приемник. Развернутая модель приемника представлена на рисунке 7.21.

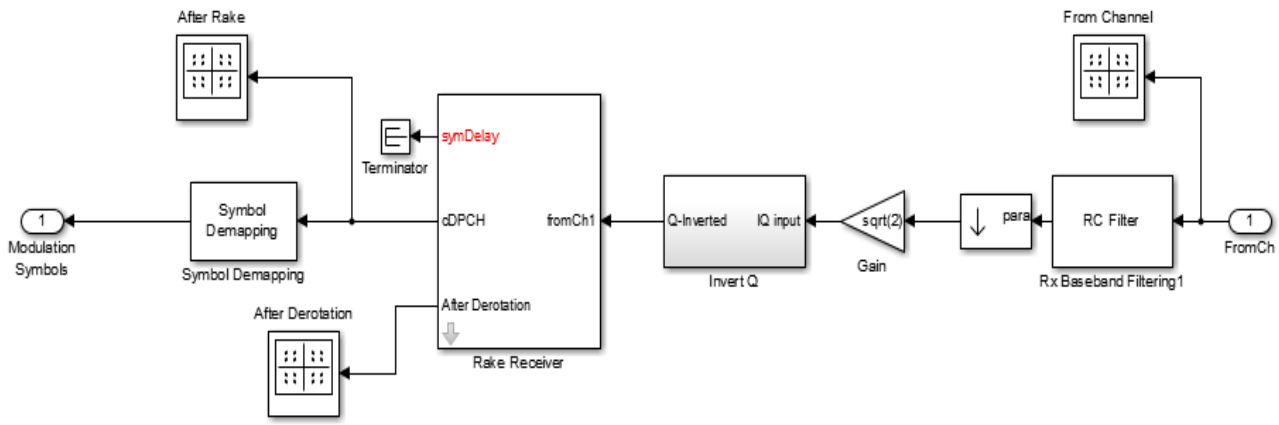


Рис. 7.21. Модель приемника

Принятый сигнал поступает на фильтр RC Filter, АЧХ которого представлена на рисунке 6, и затем усиливается с помощью блока Gain в корень из двух раз, после чего сигнал поступает в блок Invert Q, который разделяет его на реальную и мнимую части, умножает мнимую часть на -1 и затем объединяет реальную и мнимую части обратно. Далее восстанавливается созвездие с помощью блока Rake Reciever, после чего сигнал поступает в блок Symbol Demapping для демодуляции. Полученные символы модуляции поступают на декодер, развернутая модель которого представлена на рисунке 5.22.

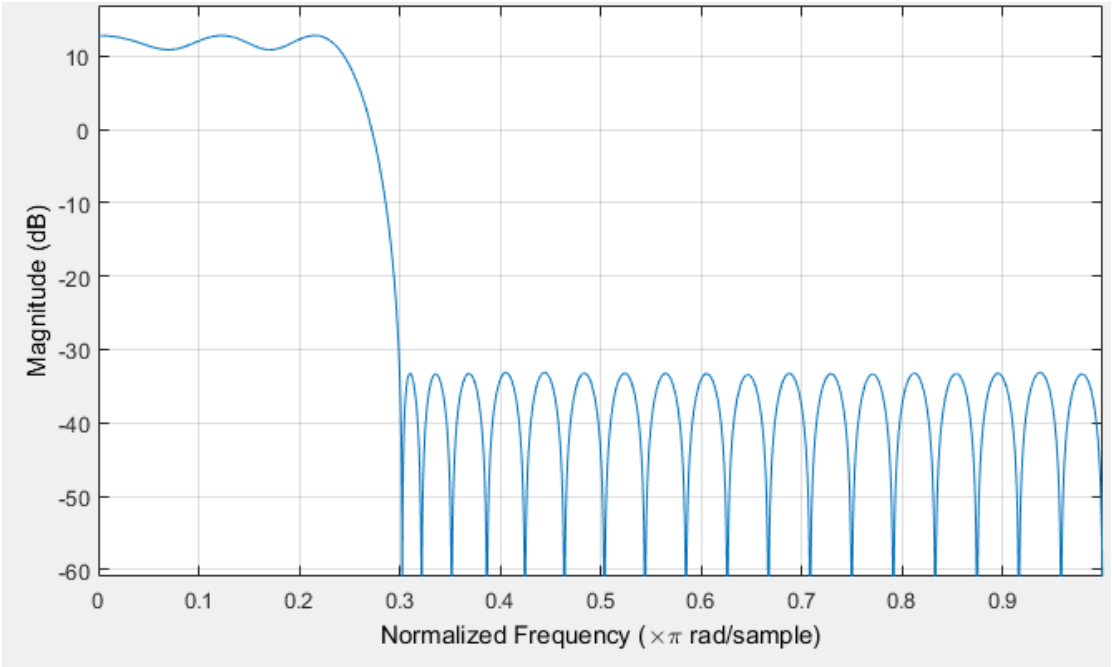


Рис. 7.22. АЧХ фильтра приемника

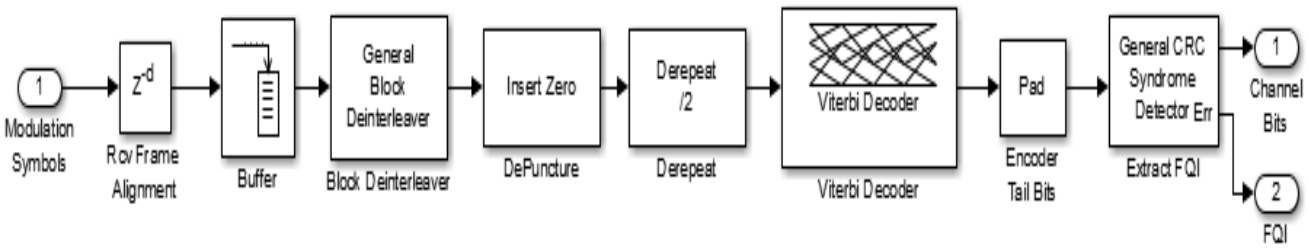


Рис. 7.23. Модель декодера.

Полученные символы модуляции поступают в блок Rcv Frame Alignment, который представляет собой задержку на 768 тактов, далее символы поступают в блок Buffer для накопления 768 символов. Накопленные символы поступают в блок Block Deinterleaver для обратного перемежения, далее данные поступают в блок Insert Zero, который возвращает последовательности нулей, замененных на специальные символы, далее данные поступают в блок Derepeat, обратное преобразование кодов с повторением с коэффициентом повторения 2, далее данные поступают на декодер Витерби и наконец в блок Encoder Tail Bits, который добавляет нули или урезает число бит если оно не равно 80.

Параметры модели

Модель позволяет изменять такие настройки как скорость потока и вид канала. В зависимости от вида канала можно задавать значение отношения сигнал/шум, а также параметры многолучевого распространения сигнала: максимальное Доплеровское отклонение частоты, вектор задержки и вектор ослабления/усиления. Длины векторов определяют количество лучей в канале.

Результаты моделирования

Компонент расчета BER сравнивает декодированный сигнал и сигнал, сгенерированный базовой станцией. Если BER равен нулю, то сигнал не подвергся каким-либо изменениям либо ошибки удалось исправить. Сигнал с базовой станции перед попаданием в блок расчета BER проходит через задержку для того что бы выровнять фреймы.

Для того что бы отобразить все возможные графики необходимо два раза кликнуть по кнопке Open Scopes в правом верхнем углу. В результате чего отобразятся следующие графики:

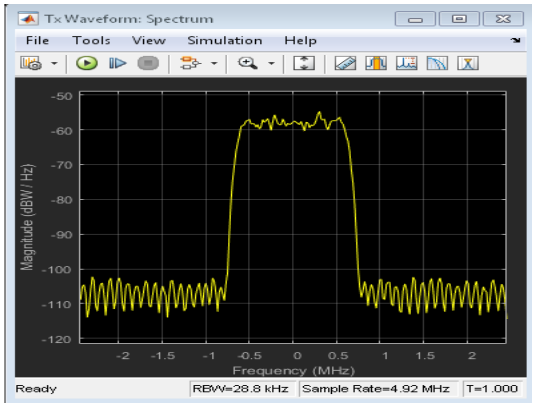


Рис. 7.24. Спектр сигнала сгенерированного базовой станцией.

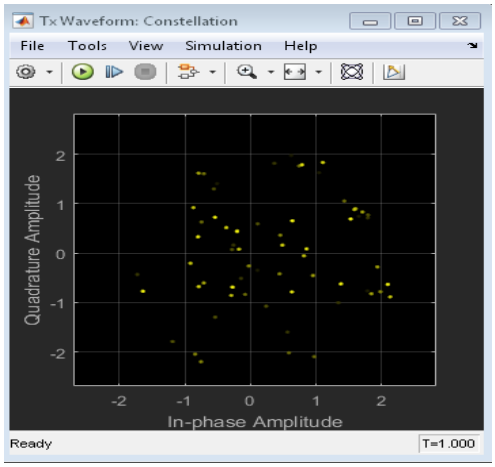


Рис. 7.25. Сгенерированный базовой станцией сигнал на I-Q диаграмме

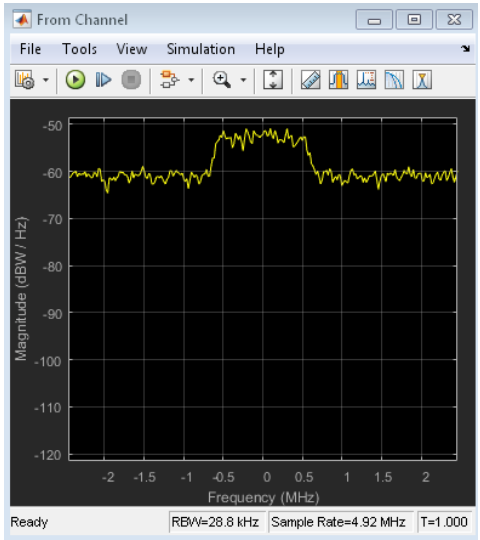


Рис. 7.26. Спектр принимаемого мобильной станцией сигнала после прохождения через канал

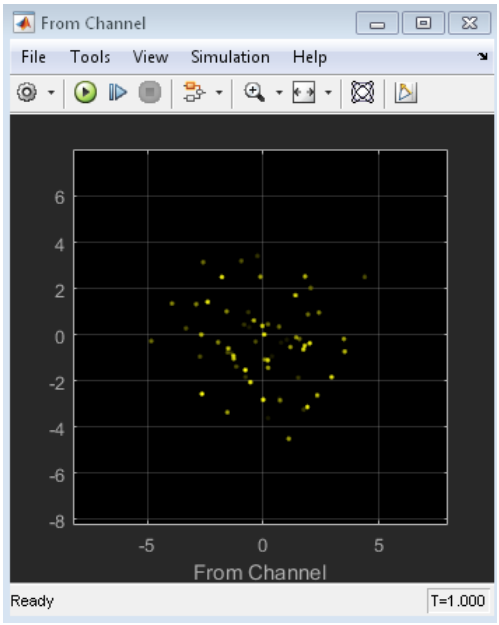


Рис. 7.27. Сигнал принимаемый мобильной станцией после прохождения через канал на I-Q диаграмме.

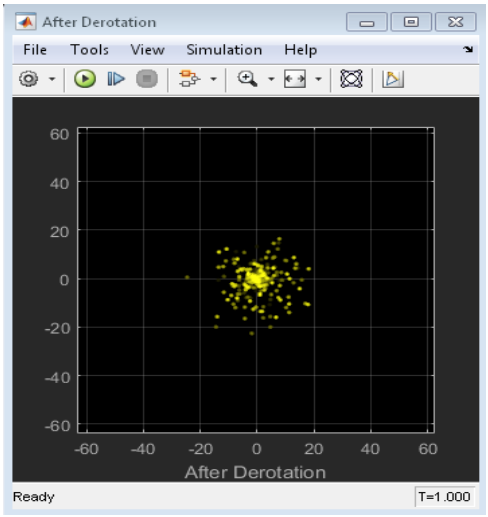


Рис. 7.28. Сигнал, принятый мобильной станцией

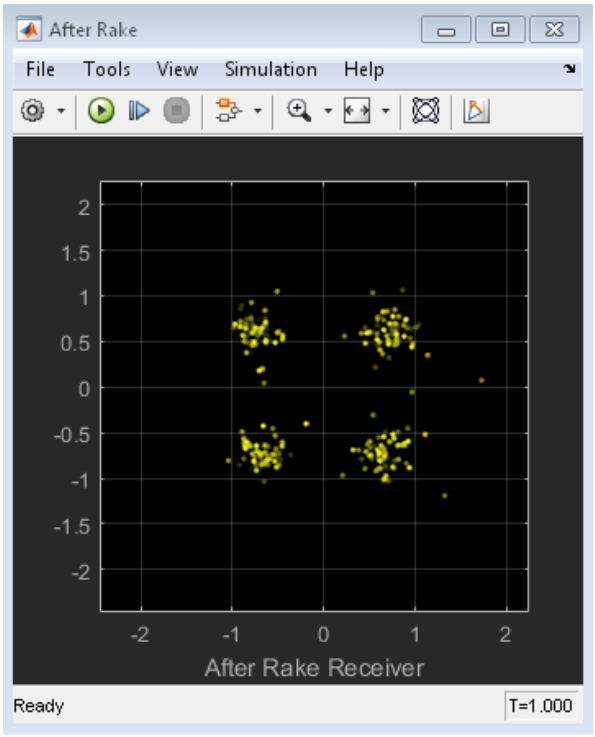


Рис. 7.29. Сигнал, декодированный мобильной станцией, на I-Q диаграмме.

Исследование модели

В блоке Model Parameters во вкладке Channel Settings выберем Channel Model: No Channel.

Результат моделирования:

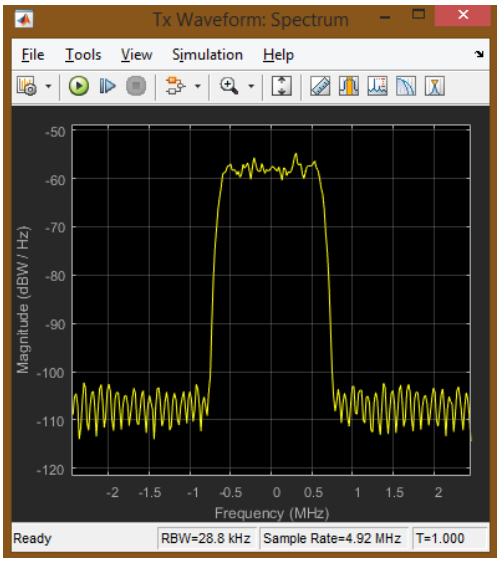


Рис. 7.30. Спектр сигнала сгенерированного базовой станцией

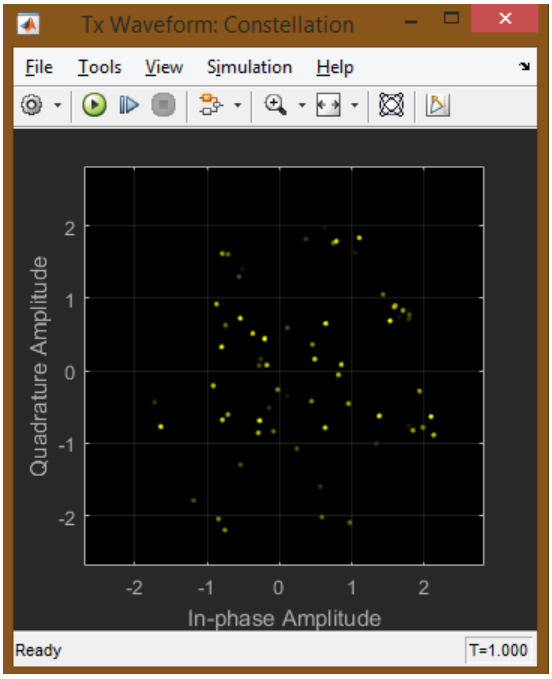


Рис. 7.31. Сгенерированный базовой станцией сигнал на I-Q диаграмме.

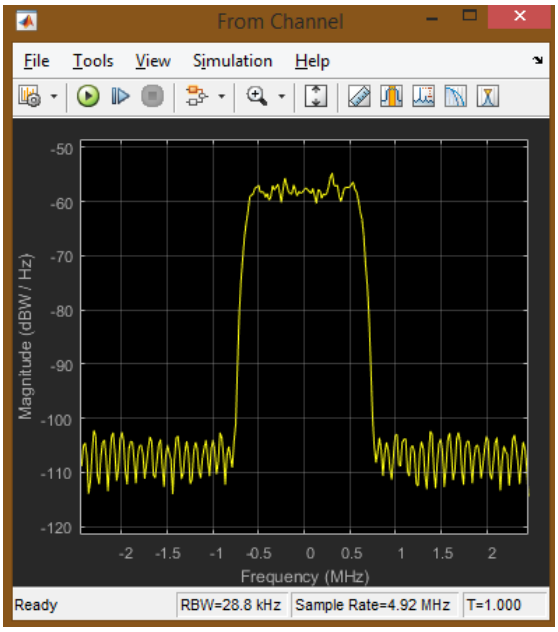


Рис. 7.32. Спектр сигнала после канала

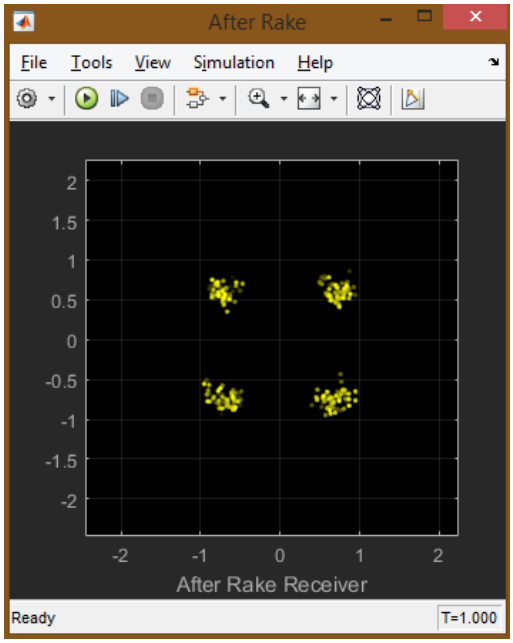


Рис. 7.33. Сигнал, декодированный мобильной станцией, на I-Q диаграмме

Видно, что спектр сигнала не изменился, так как в канале не было потерь. По результатам моделирования BER равен нулю.

В блоке Model Parameters во вкладке Channel Settings выберем Channel Model: AWGN Channel.

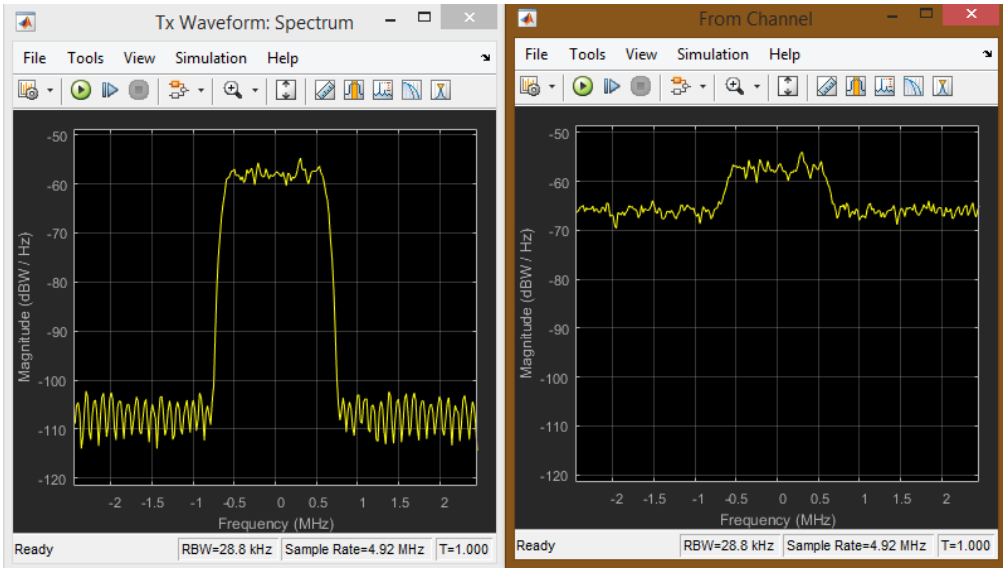


Рис. 7.34. Спектр сигнала до и после канала при отношении сигнал/шум 5 дБ

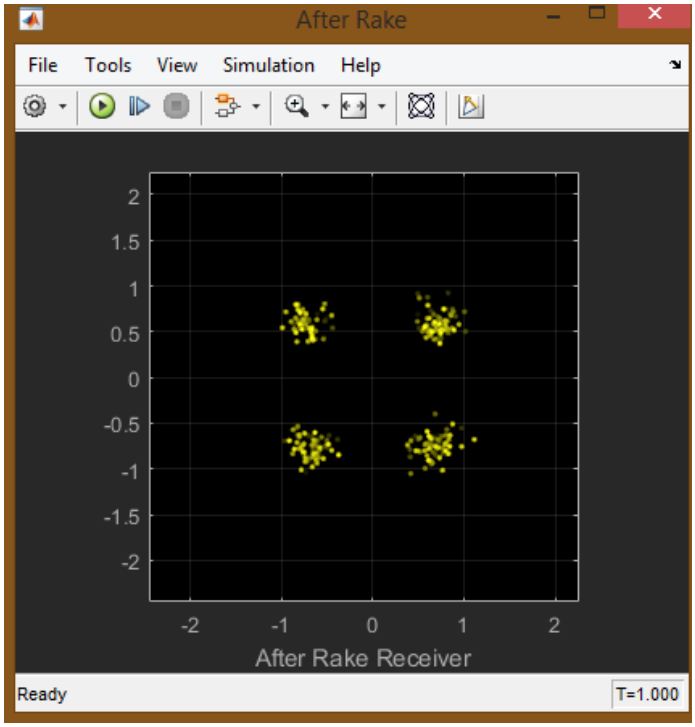


Рис. 7.35. Сигнал, декодированный мобильной станцией, на I-Q диаграмме.

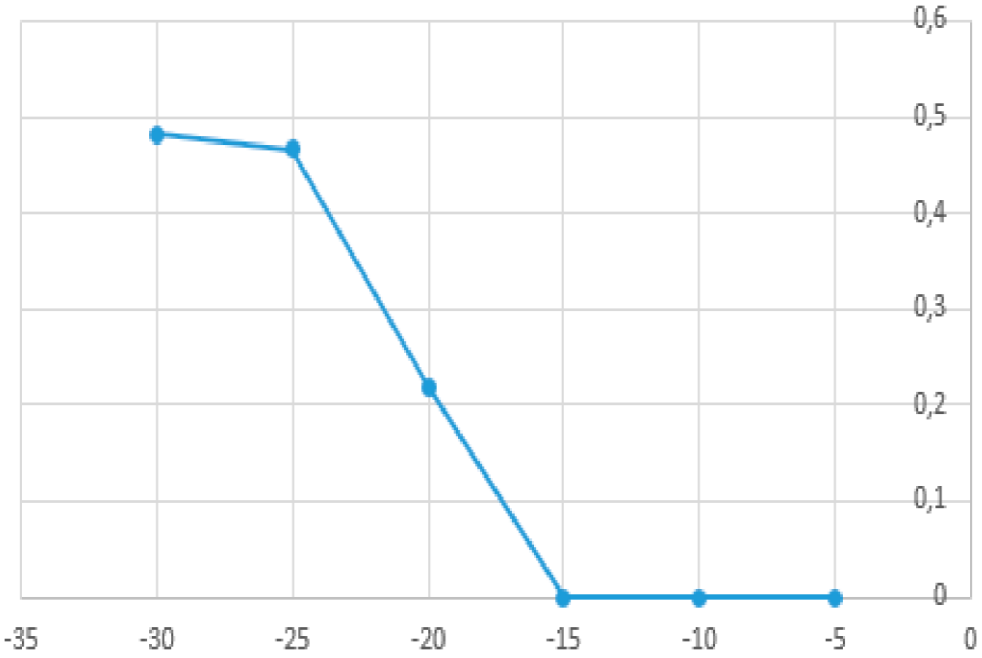


Рис. 7.36. Зависимость BER от SNR в канале с шумами.

Таблица 7.1. Зависимость BER от SNR в канале с шумами.

SNR	-30	-25	-20	-15	-10	-5
BER	0,4814	0,4662	0,2186	0	0	0

В блоке Model Parameters во вкладке Channel Settings выберем Channel Model: Multipath Fading Channel.

И установим следующие параметры

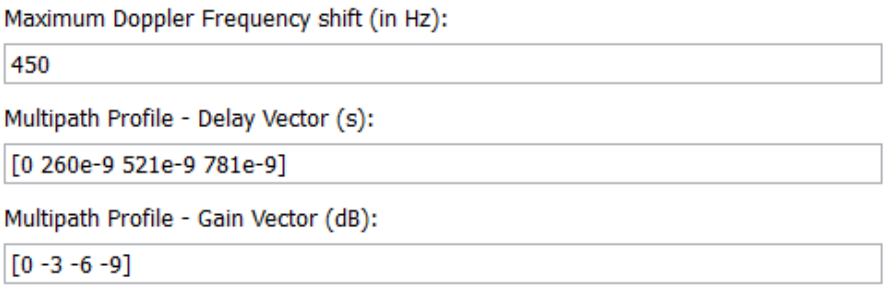


Рис. 7.37. Заданные параметры канала с многолучевым распространением.

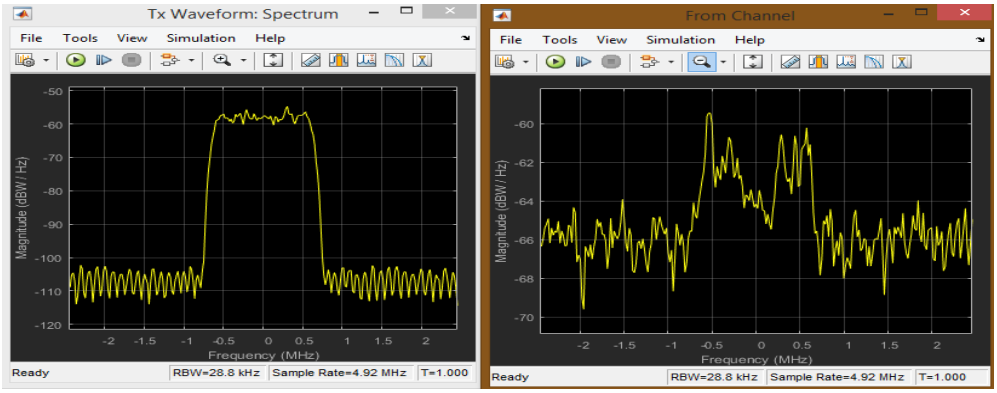


Рис. 7.38. Спектры сигнала до и после канала при отношении сигнал/шум 5 дБ.

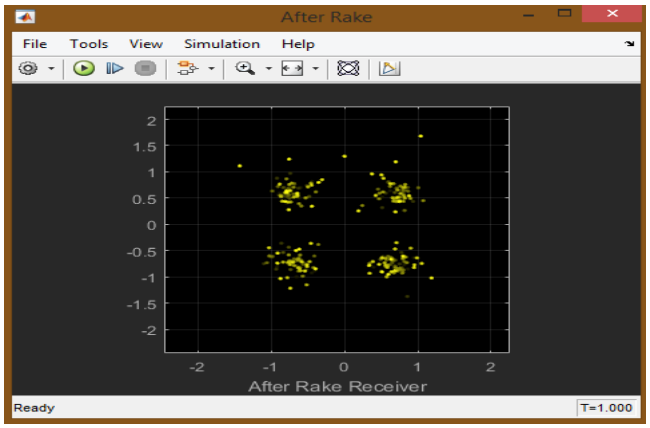


Рис. 7.39. Сигнал, декодированный мобильной станцией, на I-Q диаграмме.

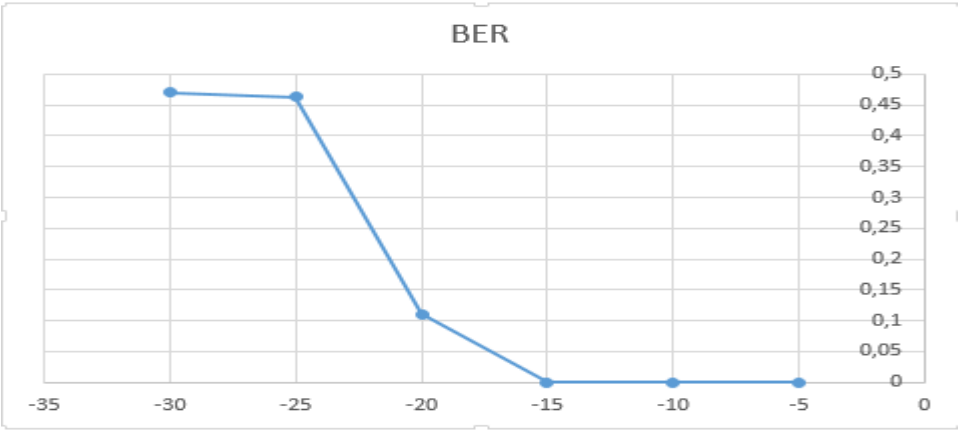


Рис. 7.40. Зависимость BER от SNR в канале с многолучевым распространением.

Таблица 7.2. Зависимость BER от SNR в канале с многолучевым распространением

SNR	-30	-25	-20	-15	-10	-5

BER	0,4708	0,4637	0,1105	0	0	0

В блоке Model Parameters во вкладк*е Channel Settings выберем Channel Model: Multipath Fading Channel.

И установим следующие параметры

Maximum Doppler Frequency shift (in Hz):

600

Multipath Profile - Delay Vector (s):

[0 280e-9 541e-9 801e-9]

Multipath Profile - Gain Vector (dB):

[0 -4 -7 -10]

Рис. 7.41. Заданные параметры канала с многолучевым распространением

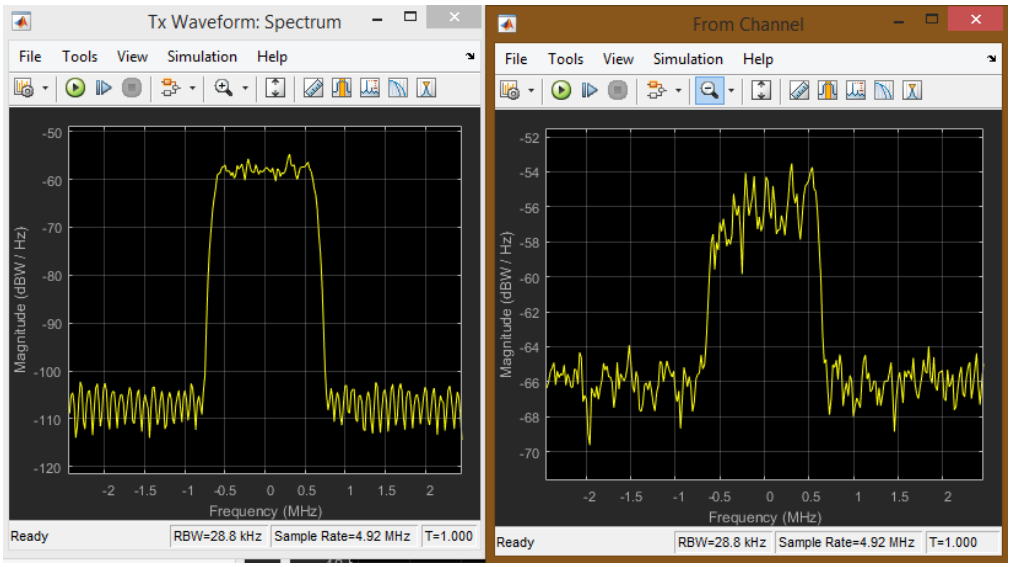


Рис. 7.42. Спектры сигнала до и после канала при отношении сигнал/шум 5 дБ

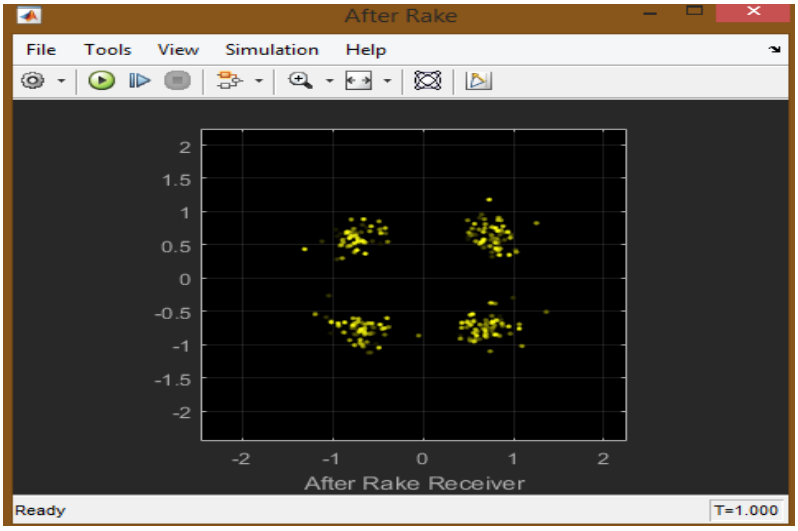


Рис. 7.43. Сигнал, декодированный мобильной станцией, на I-Q диаграмме

Таблица 7.3. Зависимость BER от SNR в канале с многолучевым распространением

SNR	-30	-25	-20	-15	-10	-5
BER	0,5007	0,4657	0,1532	0	0	0

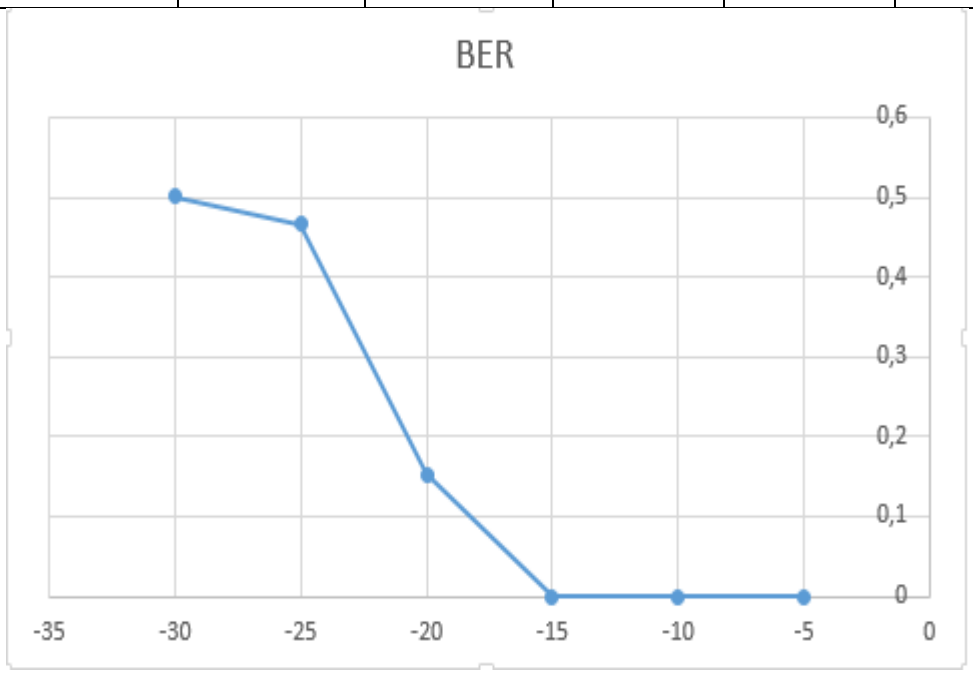


Рис. 7.44. Зависимость BER от SNR в канале с многолучевым распространением

Таким образом, в разделе было сделано:

Проведен аналитический обзор существующих методов и средств систем мобильной связи с кодовым разделением канала CDMA;

Разработана структурная схема DownLink канала CDMA2000 и приведена в приложении Б;

Приведена модель DownLink канала CDMA2000 реализованная в MATLAB R2015b;

Приведено исследование данной модели, а также методика проведения исследования, представленная в приложении А. Данную методику можно использовать для проведения учебных лабораторных работ.

На основе проведенного исследования можно сделать следующие выводы:

Система мобильной связи CDMA2000 обладает рядом преимуществ: возможность декодировать сигналы при отношении сигнал/шум меньше единицы, т.е. уровень передаваемого сигнала ниже уровня шума, что делает сигнал скрытным, а значит более защищенным.

Формируемый сигнал возможно принять и декодировать без ошибок даже при наличии многолучевости, однако при большом Доплеровском отклонении частоты и больших задержках, например, 1МГц и 1 мкс ошибки будут даже при высоком отношении сигнал/шум, например, 40 дБ. Но такие плохие характеристики канала довольно редки.

Для большей защищенности в аппаратуре стандарта CDMA длинный код формируется в результате нескольких последовательных логических операций с псевдослучайной двоичной последовательностью, генерируемой в 42-разрядном регистре сдвига, и двоичной 32-битовой маской, которая определяется индивидуально для каждого абонента. Такой регистр сдвига применяется во всех базовых станциях этого стандарта для обеспечения режима синхронизации всей сети. Длина М-последовательности при этом составляет 4 398 046 511 103 бит и если ее элементы формируются с тактовой частотой, например, 450 МГц, то период повторения будет составлять 9773,44 с= 2 ч 43 мин. Это значит, что если даже удастся засинхронизировать приемник в случае несанкционированного перехвата, то чтобы определить структуру сигнала-носителя необходимо вести наблюдение в течение почти 3-х часов, а с применением индивидуальной 32-битовой маски 'подслушивание" практически исключено.

Таблица 7.4. Характеристики CDMA2000

Характеристика	Значение
Базовая скорость передачи данных в канале	9.6 кбит/с
Длительность пакетов, на которые разбивается базовый поток	20 мс
Цифровая модуляция DownLink	QPSK
Цифровая модуляция UpLink	OQPSK
Размер матрицы Адамара	64x64
Разрядность регистра сдвига для	42

формирования длинного кода	
Длина М-последовательности длинного кода	4 398 046 511 103
Количество бит в индивидуальной маске пользователя	32
Разрядность регистра сдвига для формирования короткого кода	15
Длина М-последовательности короткого кода	32768
Частота среза КИХ-фильтра	615 кГц

Методика проведения измерений работы:

Запустить MATLAB R2015b от имени администратора;

В командной строке ввести команду «cdma2000SimulinkExample»;

Два раза кликнуть левой кнопкой мыши по блоку Model Parameters;

Во вкладке Channel Settings выбрать Channel Model: No Channel;

Два раза кликнуть левой кнопкой мыши по блоку Open Scopes;

Запустить моделирование;

После отображения всех графиков сохранить полученные данные и убедиться, что спектр сигнала, до и после канала, не изменился;

Не закрывая окна с графиками два раза кликнуть левой кнопкой мыши по блоку Model Parameters;

Во вкладке Channel Settings выбрать Channel Model: AWGN Channel и изменяя значение отношения сигнал/шум построить зависимость BER от SNR, и сохранить полученные диаграммы хотя бы для одного измерения;

Не закрывая окна с графиками два раза кликнуть левой кнопкой мыши по блоку Model Parameters;

Во вкладке Channel Settings выбрать Channel Model: Multipath Fading Channel и изменяя значение отношения сигнал/шум построить зависимость BER от SNR, и сохранить полученные диаграммы хотя бы для одного измерения;

Не закрывая окна с графиками два раза кликнуть левой кнопкой мыши по блоку Model Parameters;

Во вкладке Channel Settings изменить параметры доплеровского отклонения частоты (Maximum Doppler Frequency shift), вектора задержки (Multipath Profile – Delay Vector),

вектора усиления (Multipath Profile – Gain Vector) и повторить пункт 11. Длины векторов задержки и усиления должны совпадать.

7.3. Системы мобильной связи стандарта IEEE 802.11 (WiFi)

На современном этапе развития сетевых технологий, технология беспроводных сетей Wi-Fi является наиболее удобной в условиях, требующих мобильность, простоту установки и использования. Как правило, технология Wi-Fi используется для организации беспроводных локальных компьютерных сетей, а также создания так называемых горячих точек высокоскоростного доступа в Интернет.

Беспроводные сети обладают, по сравнению с традиционными проводными сетями, немалыми преимуществами, главным из которых, конечно же, является:

Простота развёртывания;

Гибкость архитектуры сети, когда обеспечивается возможность динамического изменения топологии сети при подключении, передвижении и отключении мобильных пользователей без значительных потерь времени;

Быстрота проектирования и реализации, что критично при жестких требованиях к времени построения сети;

В то же время беспроводные сети на современном этапе их развития не лишены серьёзных недостатков. Прежде всего, это зависимость скорости соединения и радиуса действия от наличия преград и от расстояния между приёмником и передатчиком. Один из способов увеличения радиуса действия беспроводной сети заключается в создании распределённой сети на основе нескольких точек беспроводного доступа. При создании таких сетей появляется возможность превратить здание в единую беспроводную зону и увеличить скорость соединения вне зависимости от количества стен (преград). Аналогично решается и проблема масштабируемости сети, а использование внешних направленных антенн позволяет эффективно решать проблему препятствий, ограничивающих сигнал.

В соответствии с техническим заданием основными задачами данной работы являлись:

1. Аналитический обзор существующих методов и средств;

2. Разработка структурной схемы программного комплекса;

3. Разработка алгоритма программы;

4. Разработка программного интерфейса для исследования характеристик и визуализации основных преобразований;

5. Разработка методики и проведение исследования основных технических характеристик, анализ результатов исследования.

Полученная в результате разработка позволяет исследовать беспроводные сети на базе стандарта 802.11b.

История развития

В 1990 г. Комитет по стандартам IEEE 802 (Institute of Electrical and Electronic Engineers) сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11. Это группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2.4 ГГц со скоростями 1 и 2 Мбит/с. Работа по созданию стандарта были завершены через семь лет, и в июне 1997 г. была ратифицирована первая спецификация 802.11 [1].

Стандарт IEEE 802.11 стал первым стандартом для продуктов WLAN от независимой международной организации. Однако к моменту выхода стандарта в свет первоначально заложенная в нем скорость передачи данных оказалась недостаточной. Это послужило причиной последующих доработок, поэтому сегодня можно говорить о группе стандартов.

Методы построения радиосигнала в WiFi-сетях

В настоящее время при разработке аппаратуры для беспроводных сетей используются два метода построения сигнала:

С непосредственной модуляцией несущей частоты (Direct-Sequence Spread Spectrum – DSSS).

Информационный сигнал домножается на псевдослучайный код (Pncode – Pseudo Random Noise Code). Полученный результат используют для модуляции несущей. В приемнике полученный сигнал умножают на тот же код и выделяют полезный сигнал.

Основной проблемой, возникающей при использовании метода прямой последовательности, является эффект близко расположенного передатчика, т.е. уровень сигнала мешающего передатчика гораздо выше уровня нужного передатчика, что может привести к потери связи.

Со скачкообразной перестройкой частоты (Frequency-Hopping Spread Spectrum – FHSS).

Частота несущей изменяется согласно уникальной последовательности. Для реализации этого метода необходим скоростной синтезатор частот.

Недостаток: сложность получения высокого значения базы сигнала, что необходимо для увеличения числа пользователей, помехоустойчивости, повышения конфиденциальности.

Достоинство: меньшая подверженность эффекту близкого передатчика.

Оба метода основаны на принципе приемопередачи с «расширенным спектром», который обеспечивает защиту от помех и конфиденциальность передаваемой информации. Обычно при выборе сетевого продукта учитывают следующие факторы: скорость передачи данных, дальность устойчивой связи, соответствие стандартам, эксплуатационные характеристики и

стоимость. Выбор типа аппаратуры для беспроводной сети определяется как условиями эксплуатации, так и стоимостью изделия. Следует отметить, что устройства, работающие по методу FHSS, можно получить миниатюрный и недорогой адаптер для портативного ПК [2].

Описание стандарта

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11 на практике чаще всего используются всего три стандарта, определенные Инженерным институтом электротехники и радиоэлектроники (IEEE): 802.11b, 802.11a и 802.11g.

В стандарте IEEE 802.11b благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных локальных сетей Ethernet, а также ориентации на диапазон 2,4 ГГц, этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

Поскольку оборудование, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, стандартом 802.11b предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

Стандарт IEEE 802.11a имеет большую ширину полосы из семейства стандартов 802.11 при скорости передачи данных до 54 Мбит/с.

В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM).

К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия.

Стандарт IEEE 802.11g является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому на сегодня это наиболее перспективный стандарт беспроводной связи.

При разработке стандарта 802.11g рассматривались две отчасти конкурирующие технологии: метод ортогонального частотного разделения OFDM и метод двоичного пакетного сверточного кодирования PBCC, опционально реализованный в стандарте 802.11b. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

Физические уровни стандарта

Основное назначение физических уровней стандарта 802.11 - обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Уровни MAC и PHY разрабатывались так, чтобы они были независимыми. Именно независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах802.11b, 802.11a и 802.11g.

Каждый из физических уровней стандарта 802.11 имеет два подуровня:

Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.

Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

На рис.1 показано, как эти подуровни соотносятся между собой и с вышестоящими уровнями в модели взаимодействия открытых систем (Open System Interconnection - OSI).

Подуровень PLCP по существу является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC Protocol Data Units - MPDU) между MAC-станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную среду. Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11.

Перед тем как приступить к изучению физических уровней, рассмотрим одну из составляющих физического уровня, до сих пор не упомянутую, а именно - скрэмблирование.

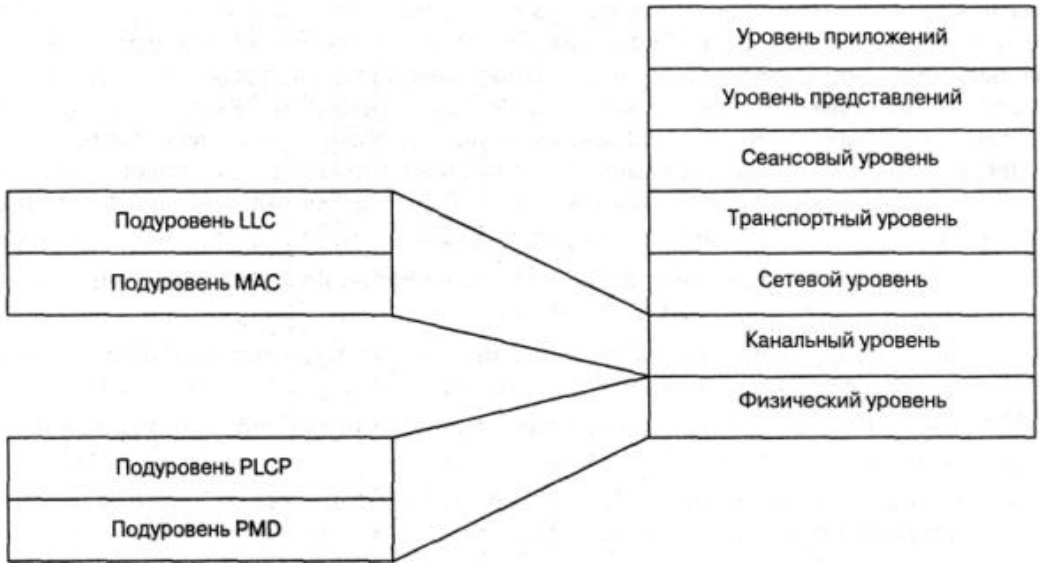


Рис. 7.45. Подуровни уровня PHY

Одна из особенностей, лежащих в основе современных передатчиков, благодаря которой данные можно передавать с высокой скоростью, - это предположение о том, что данные, которые предлагаются для передачи, поступают, с точки зрения передатчика, случайным образом. Без этого предположения многие преимущества, получаемые за счет применения остальных составляющих физического уровня, остались бы нереализованными.

Однако бывает, что принимаемые данные не вполне случайны и на самом деле могут содержать повторяющиеся наборы и длинные последовательности нулей и единиц.

Скрэмблирование (перестановка элементов) - это метод, посредством которого принимаемые данные делаются более похожими на случайные; достигается это путем перестановки битов последовательности таким образом, чтобы превратить ее из структурированной в похожую на случайную. Эту процедуру иногда называют "отбеливанием потока данных". Дескрэмблер приемника затем выполняет обратное преобразование этой случайной последовательности с целью получения исходной структурированной последовательности. Большинство способов скрэмблирования относится к числу самосинхронизирующихся; это означает, что дескрэмблер способен самостоятельно синхронизироваться со скрэмблером.

IEEE 802.11

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

Передача в диапазоне инфракрасных волн.

Технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц.

Технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

Передача в диапазоне инфракрасных волн

Средой передачи являются инфракрасные волны диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом (LED). Так как инфракрасные волны не проникают через стены, область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: ненаправленную антенну, отражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направленное излучение предназначено для организации двухточечной связи, например между двумя зданиями.

Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)

Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц

на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц, поэтому беспроводные локальные сети FHSS используют относительно высокую скорость передачи символов - 1 МГц - и намного меньшую скорость перестройки с канала на канал.

Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между шестью (6 МГц) каналами. Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков должны быть разбиты на три набора последовательностей, длина которых для Северной Америки и большей части Европы составляет 26. В таблице 1 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальное перекрытие.

По сути, схема скачкообразной перестройки частоты обеспечивает неторопливый переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему в многосотовых сетях минимизируется возможность возникновения коллизий.

Таблица 7.5 - Схема FHSS для Северной Америки и Европы

Набор	Схема скачкообразной перестройки частоты
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
3	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}

После того как уровень MAC пропускает MAC-фрейм, который в локальных беспроводных сетях FHSS называется также служебным элементом данных PLCP, или PSDU (PLCP Service Data Unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (PPDU - элемент данных протокола PLCP). На рис.2 представлен формат фрейма FHSS подуровня PLCP.

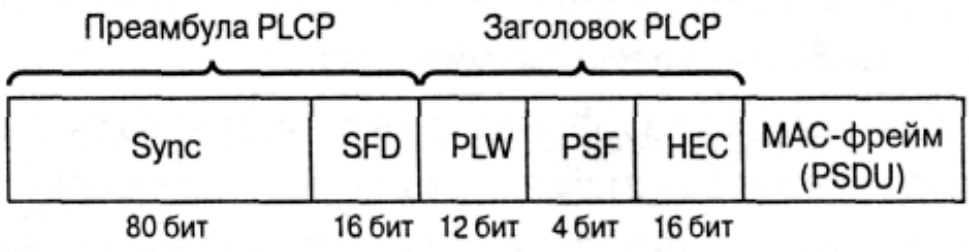


Рис. 7.46. Формат фрейма FHSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

Подполе Sync размером 80 бит. Строка, состоящая из чередующихся 0 и 1, начинается с 0. Приемная станция использует это поле, чтобы принять решение о выборе антенны при наличии такой возможности, откорректировать уход частоты (frequency offset) и синхронизировать распределение пакетов (packet timing).

Подполе флага начала фрейма (Start of Frame Delimiter, SFD) размером 16 бит. Состоит из специфической строки (0000 1100 1011 1101, крайний слева бит первый) в обеспечение синхронизации фреймов (frame timing) для приемной станции.

Заголовок фрейма PLCP состоит из трех подполей:

Слово длины служебного элемента данных PLCP (PSDU), PSDU Length Word (PLW) размером 12 бит. Указывает размер фрейма MAC (PSDU) в октетах.

Сигнальное поле PLCP (Signaling Field PLCP - PSF) размером 4 бит. Указывает скорость передачи данных конкретного фрейма.

HEC (Header Error Check). Контрольная сумма фрейма.

Служебный элемент данных PLCP (PSDU) проходит через операцию скрэмблирования с целью отбеливания (рандомизации) последовательности входных битов. Получившийся в результате PSDU представлен на рис.3. Заполняющие символы вставляются между всеми 32-символьными блоками. Эти заполняющие символы устраняют любые систематические отклонения в данных, например, когда единиц больше, чем нулей, или наоборот, которые могли бы привести к нежелательным эффектам при дальнейшей обработке.

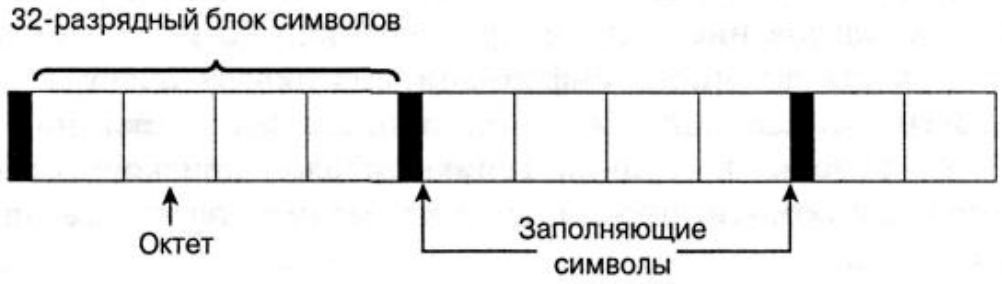


Рис. 7.47. Скрэмблированный PSDU в технологии FHSS

Подуровень PLCP преобразует фрейм в поток битов и передает его на подуровень PMD. Подуровень PMD технологии FHSS модулирует поток данных с использованием модуляции, основанной на гауссовой частотной модуляции (Gaussian Frequency Shift Keying - GFSK).

Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности

В спецификации стандарта 802.11 оговорено использование и другого физического уровня - на основе технологии широкополосной модуляции с расширением спектра методом прямой

последовательности (DSSS). Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с.

Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLCP технологии DSSS стандарта 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLCP и заголовок PLCP Формат фрейма представлен на рис.7.48.

Рис. 7.48. Формат фрейма DSSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого подполя - обеспечить синхронизацию для приемной станции.

Подполе SFD шириной 16 бит ; в нем содержится специфичная строка OxF3A0; его задача - обеспечить тайминг (timing) для приемной станции.

Заголовок PLCP состоит из четырех подполей:

Подполе Signal шириной 8 бит, указывающее тип модуляции и скорость передачи для данного фрейма.

Подполе Service шириной 8 бит зарезервировано. Это означает, что во время разработки спецификации стандарта оно осталось неопределенным; предполагается, что оно пригодится в будущих модификациях стандарта.

Подполе Length шириной 16 бит, указывающее количество микросекунд (из диапазона 16-216), необходимое для передачи части MAC-фрейма.

Подполе CRC. 16-битная контрольная сумма.

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скрэмблирования с целью рандомизации данных.

Скрэмблированная преамбула PLCP всегда передается со скоростью 1 Мбит/с, в то время как скрэмблированный фрейм MPDU передается со скоростью, указанной в подполе Signal. Подуровень PMD модулирует отбеленный поток битов, используя следующиеметоды модуляции:

Двоичная относительная фазовая модуляция (Differential Binary Phase Shift Keying - DBPSK) для скорости передачи 1 Мбит/с.

Квадратурная относительная фазовая модуляция (Differential Quadrature Phase Shift Key - DQPSK) для скорости передачи 2 Мбит/с.

IEEE 802.11b

На физическом уровне к MAC-кадрам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка.

Преамбула содержит стартовую синхропоследовательность (SYNC) для настройки приемника и 16-битный код начала кадра (SFD) - число F3A016. PLCP-заголовок включает поля SIGNAL (информация о скорости и типе модуляции), SERVICE (дополнительная информация, в том числе о применении высокоскоростных расширений и PBCC-модуляции) и LENGTH (время в микросекундах, необходимое для передачи следующей за заголовком части кадра). Все три поля заголовка защищены 16-битной контрольной суммой CRC.

Рис. 7.49. Структура кадров сети IEEE 802.11b физического уровня

В стандарте IEEE 802.11b предусмотрено два типа заголовков: длинный и короткий (51).

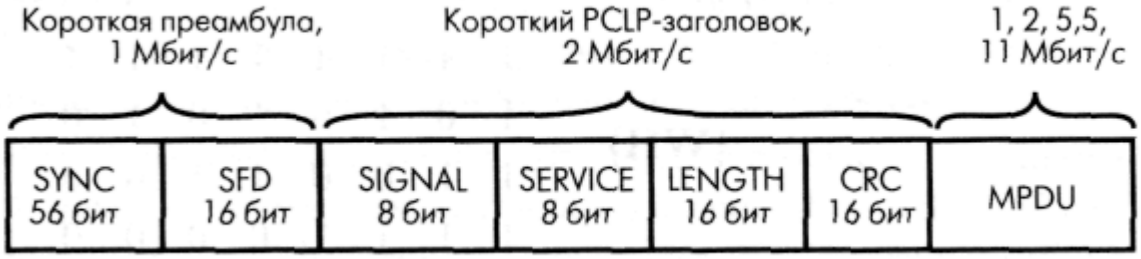


Рис. 7.50. Короткий заголовок кадров сети 802.11b

Они отличаются длиной синхропоследовательности (128 и 56 бит), способом ее генерации, а также тем, что символ начала кадра в коротком заголовке передается в обратном порядке. Кроме того, если все поля длинного заголовка передаются со скоростью 1 Мбит/с, то при коротком заголовке преамбула транслируется на скорости 1 Мбит/с, другие

поля заголовка - со скоростью 2 Мбит/с. Остальную часть кадра можно передавать на любой из допустимых стандартом скоростей передачи, указанных в полях SIGNAL и SERVICE. Короткие заголовки физического уровня предусмотрены спецификацией IEEE 802.11b для увеличения пропускной способности сети.

Из описания процедур связи сети IEEE 802.11 видно, что "накладные расходы" в этом стандарте выше, чем в проводной сети Ethernet. Поэтому крайне важно обеспечить высокую скорость передачи данных в канале. Повысить пропускную способность канала с заданной шириной полосы частот можно, разрабатывая и применяя новые методы модуляции. По этому пути пошла группа разработчиков IEEE 802.11b.

Напомним, что изначально стандарт IEEE 802.11 предусматривал работу в режиме DSSS с использованием так называемой Баркеровской последовательности (Barker) длиной 11 бит: B1 = (10110111000). Каждый информационный бит замещается своим произведением по модулю 2 (операция "исключающее ИЛИ") с данной последовательностью, т. е. каждая информационная единица заменяется на B1, каждый ноль - на инверсию B1. В результате бит заменяется последовательностью 11 чипов. Далее сигнал кодируется посредством дифференциальной двух- или четырехпозиционной фазовой модуляции (DBPSK или DQPSK, один или два чипа на символ соответственно). При частоте модуляции несущей 11 МГц общая скорость составляет в зависимости от типа модуляции 1 и 2 Мбит/с.

Стандарт IEEE 802.11b дополнительно предусматривает скорости передачи 11 и 5,5 Мбит/с. Для этого используется так называемая ССК-модуляция (Complementary Code Keying - кодирование комплементарным кодом).

Хотя механизм расширения спектра, используемый для получения скоростей 5,5 и 11 Мбит/с с применением ССК, относится к методам, которые применяются для скоростей 1 и 2 Мбит/с, он по-своему уникален. В обоих случаях применяется метод расширения, но при использовании модуляции ССК расширяющий код представляет собой код из 8 комплексных чипов, в то время как при работе со скоростями 1 и 2 Мбит/с применяется 11-разрядный код. 8-чиповый код определяется или 4, или 8 битами - в зависимости от скорости передачи данных. Скорость передачи чипов составляет 11 Мчип/с, т.е. при 8 комплексных чипах на символ и 4 или 8 битов на символ можно добиться скорости передачи данных 5,5 и 11 Мбит/с.

Для того чтобы передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать скрэмблированный поток битов в символы по 4 бита (b0, b1, b2 и b3). Последние два бита (b2 и b3) используются для определения 8 последовательностей комплексных чипов, как показано в таблице 6, где {cl, c2, c3, c4, c5, c6, c7, c8} представляют чипы

последовательности. В таблицн 6 j представляет мнимое число, корень квадратный из -1, и откладывается по мнимой, или квадратурной, оси комплексной плоскости.

Таблица 3.6. Последовательность чипов ССК								
(b2, b3)	1	2	3	4	5	6	7	C8
00				1			1	1
01	j	1	j				j	1
10	j		j	1	j			1
11		1			j			1

Теперь, имея последовательность чипов, определенную битами (b2, b3), можно использовать первые два бита (b0, b1) для определения поворота фазы, осуществляемого при модуляции по методу DQPSK, который будет применен к последовательности (таблица 3). Вы должны также пронумеровать каждый 4-битовый символ PSDU, начиная с 0, чтобы можно было определить, преобразуете вы четный либо нечетный символ в соответствии с этой таблицей. Следует помнить, что речь идет об использовании DQPSK, а не QPSK, и поэтому представленные в таблице изменения фазы отсчитываются по отношению к предыдущему символу или, в случае первого символа PSDU, по отношению к последнему символу предыдущего DQPSK-символа, передаваемого со скоростью 2 Мбит/с.

Таблица 3.7. Поворот фазы при модуляции ССК		
(b0, b1)	Изменение фазы четных символов	Изменение фазы нечетных символов
00	0	π
01	$\pi/2$	$-\pi/2$
11	π	0
10	$-\pi/2$	$\pi/2$

Это вращение фазы применяется по отношению к 8 комплексным чипам символа, затем осуществляется модуляция на подходящей несущей частоте.

Чтобы передавать данные со скоростью 11 Мбит/с, скрэмблированная последовательность битов PSDU разбивается на группы по 8 символов. Последние 6 битов выбирают одну последовательность, состоящую из 8 комплексных чипов, из числа 64 возможных последовательностей, почти так же, как использовались биты (b2, b3) для выбора одной из четырех возможных последовательностей. Биты (b0,b1) используются таким же образом, как при модуляции ССК на скорости 5,5 Мбит/с для вращения фазы последовательности и дальнейшей модуляции на подходящей несущей частоте.

В чем достоинство ССК-модуляции? Дело в том, что чипы символа определяются на основе последовательностей Уолша-Адамара. Последовательности Уолша-Адамара хорошо изучены, обладают отличными автокорреляционными свойствами. Что немаловажно, каждая такая последовательность мало коррелирует сама с собой при фазовом сдвиге - очень полезное свойство при борьбе с переотраженными сигналами. Нетрудно заметить, что теоретическое операционное усиление ССК-модуляции - 3 дБ (в два раза), поскольку без кодирования QPSK-модулированный с частотой 11 Мбит/с сигнал может транслировать 22 Мбит/с. Как видно, ССК-модуляция представляет собой вид блочного кода, а потому достаточно проста при аппаратной реализации. Совокупность этих свойств и обеспечила ССК место в стандарте IEEE 802.11b в качестве обязательного вида модуляции.

На практике важно не только операционное усиление. Существенную роль играет и равномерность распределения символов в фазовом пространстве - они должны как можно дальше отстоять друг от друга, чтобы минимизировать ошибки их детектирования. И с этой точки зрения ССК-модуляция не выглядит оптимальной, ее реальное операционное усиление не превышает 2 дБ. Поэтому изначально прорабатывался другой способ модуляции - пакетное бинарное сверточное кодирование PBCC (Packet BinaryConvolutional Coding). Этот метод вошел в стандарт IEEE 802.11b как дополнительная (необязательная) опция. Механизм PBCC (5.51) позволяет добиваться в сетях IEEE 802.11b пропускной способности 5,5, 11 и 22 Мбит/с.

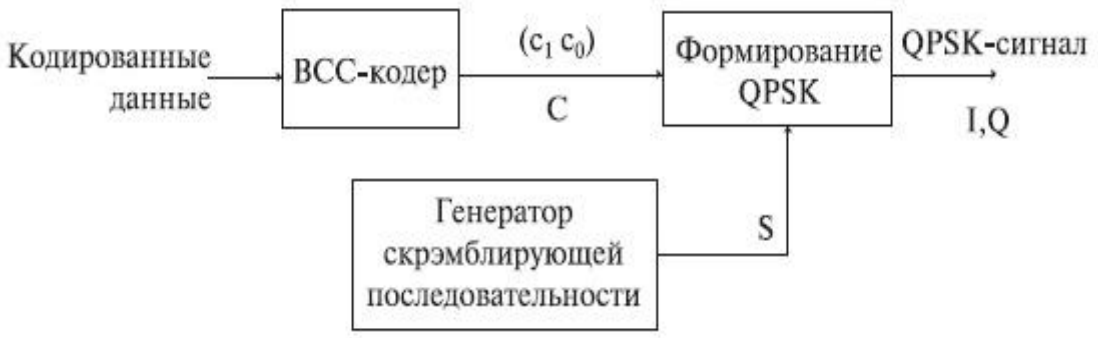


Рис. 7.51. Общая схема PBCC-модуляции

Как следует из названия, метод основан на сверточном кодировании. Для скоростей 5,5 и 11 Мбит/с поток информационных битов поступает в шестиразрядный сдвиговый регистр с сумматорами (5.52). В начальный момент времени все триггеры сдвигового регистра инициализируют нулем. В результате каждый исходный бит d заменяется двумя битами кодовой последовательности (c0, c1). При скорости 11 Мбит/с c0 и c1 задают один символ четырехпозиционной QPSK-модуляции. Для скорости 5,5 Мбит/с используют двухпозиционную BPSK-модуляцию, последовательно передавая кодовые биты c0 и c1. Если же нужна скорость 22 Мбит/с, схема кодирования усложняется (рис.5.9): три кодовых бита (c0-c2) определяют один символ в 8-позиционной 8-PSK-модуляции.

После формирования PSK-символов происходит скрэмблирование. В зависимости от сигнала s (5.51) символ остается без изменений (s = 0), либо его фаза увеличивается на $\pi/2$ (s = 1). Значение s определяет 256-битовая циклически повторяющаяся последовательность S. Она формируется на основе начального вектора U = 338Bh, в котором равное число нулей и единиц.

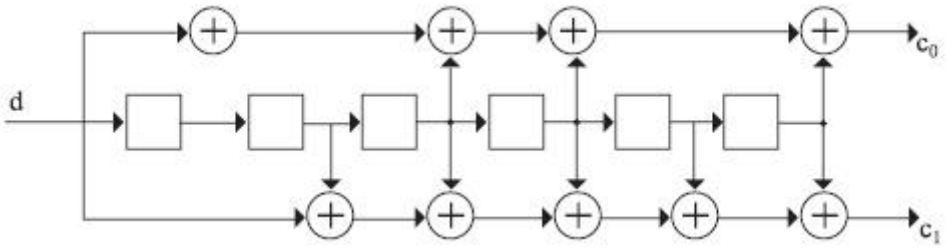


Рис. 7.52. Сверточное кодирование с двумя битами кодовой последовательности

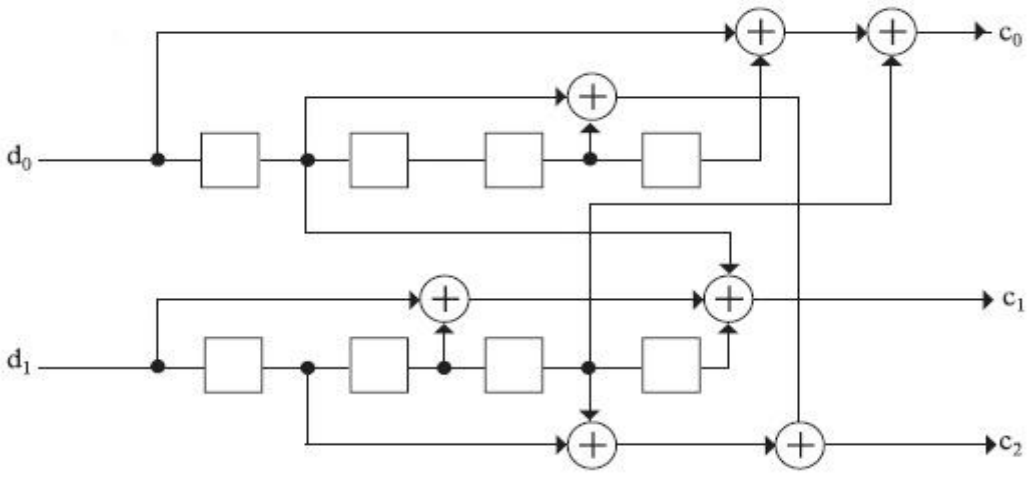


Рис. 7.53. Сверточное кодирование с тремя битами кодовой последовательности

У шестиразрядного сдвигового регистра, применяемого в PBCC для скоростей 11 и 5,5 Мбит/с, 64 возможных выходных состояния. Так что при модуляции PBCC информационные биты в фазовом пространстве оказываются гораздо дальше друг от друга, чем при CCK-модуляции. Поэтому PBCC и позволяет при одном и том же соотношении "сигнал-шум" и уровне ошибок вести передачу с большей скоростью, чем в случае CCK. Однако плата за более эффективное кодирование - сложность аппаратной реализации данного алгоритма.

IEEE 802.11a

Стандарт IEEE 802.11a появился практически одновременно с IEEE 802.11b, в сентябре 1999 года. Эта спецификация была ориентирована на работу в диапазоне 5 ГГц и основана на принципиально ином, чем описано выше, механизме кодирования данных - на частотном мультиплексировании посредством ортогональных несущих (OFDM).

Стандарт 802.11a определяет характеристики оборудования, применяемого в офисных или городских условиях, когда распространение сигнала происходит по многолучевым каналам из-за множества отражений.

В IEEE 802.11a каждый кадр передается посредством 52 ортогональных несущих, каждая с шириной полосы порядка 300 КГц (20 МГц/64). Ширина одного канала - 20 МГц. Несущие модулируют посредством BPSK, QPSK, а также 16- и 64-позиционной квадратурной амплитудной модуляции (QAM). В совокупности с различными скоростями кодирования (1/2 и 3/4, для 64-QAM - 2/3 и 3/4) образуется набор скоростей передачи 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. В таблице 5.8показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры узлов передатчика OFDM.

Таблица 7.8. Параметры передатчика стандарта 802.11a

Скорость передачи данных (Мбит/с)	Модуляция	Скорость сверточного кодирования	Число канальных битов на поднесущую	Число канальных битов на символ	Число битов данных на символ OFDM
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192

54	64-QAM	3/4	6	288	216

Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 - служебные. Структура заголовков физического уровня отличается от принятого в спецификации IEEE 802.11b, но незначительно (рис.7.54).

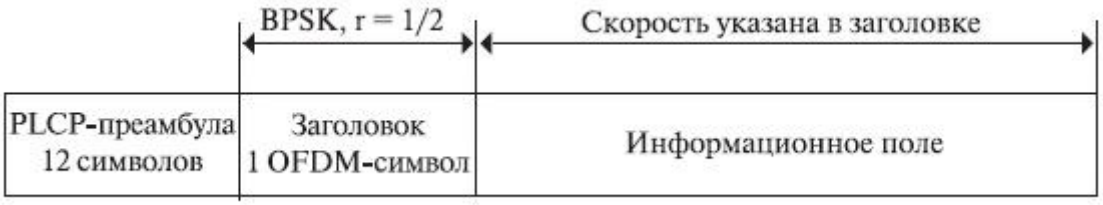


Рис. 7.54. Структура заголовка физического уровня стандарта IEEE 802.11a

Кадр включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на MAC-уровне. В заголовке передается информация о скорости кодирования, типе модуляции и длине кадра. Преамбула и заголовок транслируются с минимально возможной скоростью (BPSK, скорость кодирования r = 1/2), а информационное поле - с указанной в заголовке, как правило, максимальной, скоростью, в зависимости от условий обмена. OFDM-символы передаются через каждые 4 мкс, причем каждому символу длительностью 3,2 мкс предшествует защитный интервал 0,8 мкс (повторяющаяся часть символа). Последний необходим для борьбы с многолучевым распространением сигнала - отраженный и пришедший с задержкой символ попадет в защитный интервал и не повредит следующий символ.

Естественно, формирование/декодирование OFDM-символов происходит посредством быстрого преобразования Фурье (обратного/прямого, ОБПФ/БПФ). Функциональная схема трактов приема/передачи (рис. 5.54) достаточно стандартна для данного метода и включает сверточный кодер, механизм перемежения/перераспределения (защита от пакетных ошибок) и процессор ОБПФ. Фурье-процессор, собственно, и формирует суммарный сигнал, после чего к символу добавляется защитный интервал, окончательно формируется OFDM-символ и посредством квадратурного модулятора/конвертера переносится в заданную частотную область. При приеме все происходит в обратном порядке.

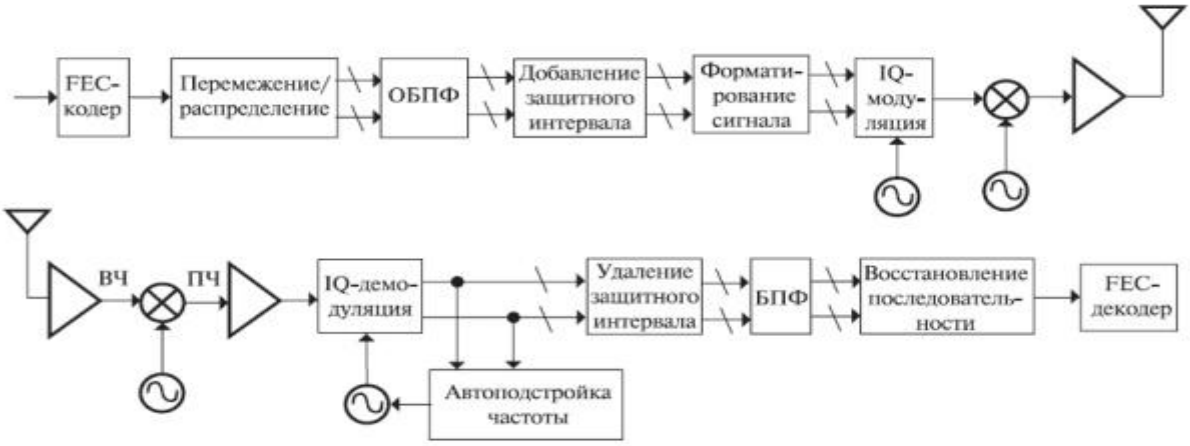


Рис. 7.55. Функциональная схема трактов приема/передачи стандарта IEEE 802.11a

IEEE 802.11g

Стандарт IEEE 802.11g по сути представляет собой перенесение схемы модуляции OFDM, прекрасно зарекомендовавшей себя в 802.11a, из диапазона 5 ГГц в область 2,4 ГГц при сохранении функциональности устройств стандарта 802.11b. Это возможно, поскольку в стандартах 802.11 ширина одного канала в диапазонах 2,4 и 5 ГГц схожа - 22 МГц.

Одним из основных требований к спецификации 802.11g была обратная совместимость с устройствами 802.11b. Действительно, в стандарте 802.11b в качестве основного способа модуляции принята схема ССК (Complementary Code Keying), а в качестве дополнительной возможности допускается модуляция PBCC (Pocket Binary Convolutional Coding).

Разработчики 802.11g предусмотрели ССК-модуляцию для скоростей до 11 Мбит/с и OFDM для более высоких скоростей. Но сети стандарта 802.11 при работе используют принцип CSMA/CA - множественный доступ к каналу связи с контролем несущей и предотвращением коллизий. Ни одно устройство 802.11 не должно начинать передачу, пока не убедится, что эфир в его диапазоне свободен от других устройств. Если в зоне слышимости окажутся устройства 802.11b и 802.11g, причем обмен будет происходить между устройствами 802.11g посредством OFDM, то оборудование 802.11b просто не поймет, что другие устройства сети ведут передачу, и попытается начать трансляцию. Последствия очевидны.

Чтобы не допустить подобной ситуации, предусмотрена возможность работы в смешанном режиме - CCK-OFDM. Информация в сетях 802.11 передается кадрами. Каждый информационный кадр включает два основных поля: преамбулу с заголовком и информационное поле (рис.5.56).

Рис. 7.56. Кадры IEEE 802.11g в различных режимах модуляции

Преамбула содержит синхропоследовательность и код начала кадра, заголовок - служебную информацию, в том числе о типе модуляции, скорости и продолжительности передачи кадра. В режиме CCK-OFDM преамбула и заголовок модулируются методом CCK (реально - путем прямого расширения спектра DSSS посредством последовательности Баркера, поэтому в стандарте 802.11g этот режим именуется DSSS-OFDM), а информационное поле - методом OFDM. Таким образом, все устройства 802.11b, постоянно "прослушивающие" эфир, принимают заголовки кадров и узнают, сколько времени будет транслироваться кадр 802.11g. В этот период они "молчат". Естественно, пропускная способность сети падает, поскольку скорость передачи преамбулы и заголовка - 1 Мбит/с.

Видимо, данный подход не устраивал лагерь сторонников технологии PBCC, и для достижения компромисса в стандарт 802.11g в качестве дополнительной возможности ввели, так же как и в 802.11b, необязательный режим - PBCC, в котором заголовок и преамбула передаются так же, как и при CCK, а информационное поле модулируется по схеме PBCC и передается на скорости 22 или 33 Мбит/с. В результате устройства стандарта 802.11g должны оказаться совместимыми со всеми модификациями оборудования 802.11b и не создавать взаимных помех. Диапазон поддерживаемых им скоростей отражен в таблице 7.9, зависимость скорости от типа модуляции - на рис.7.57.

Таблица 7.9. Возможные скорости и тип модуляции в спецификации IEEE 802.11g

Скорость, Мбит/с	Тип модуляции	
	Обязательно	Допустимо
1	Последовательность Баркера	

2	Последовательность Баркера	
5,5	CCK	PBCC
6	OFDM	OFDM
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

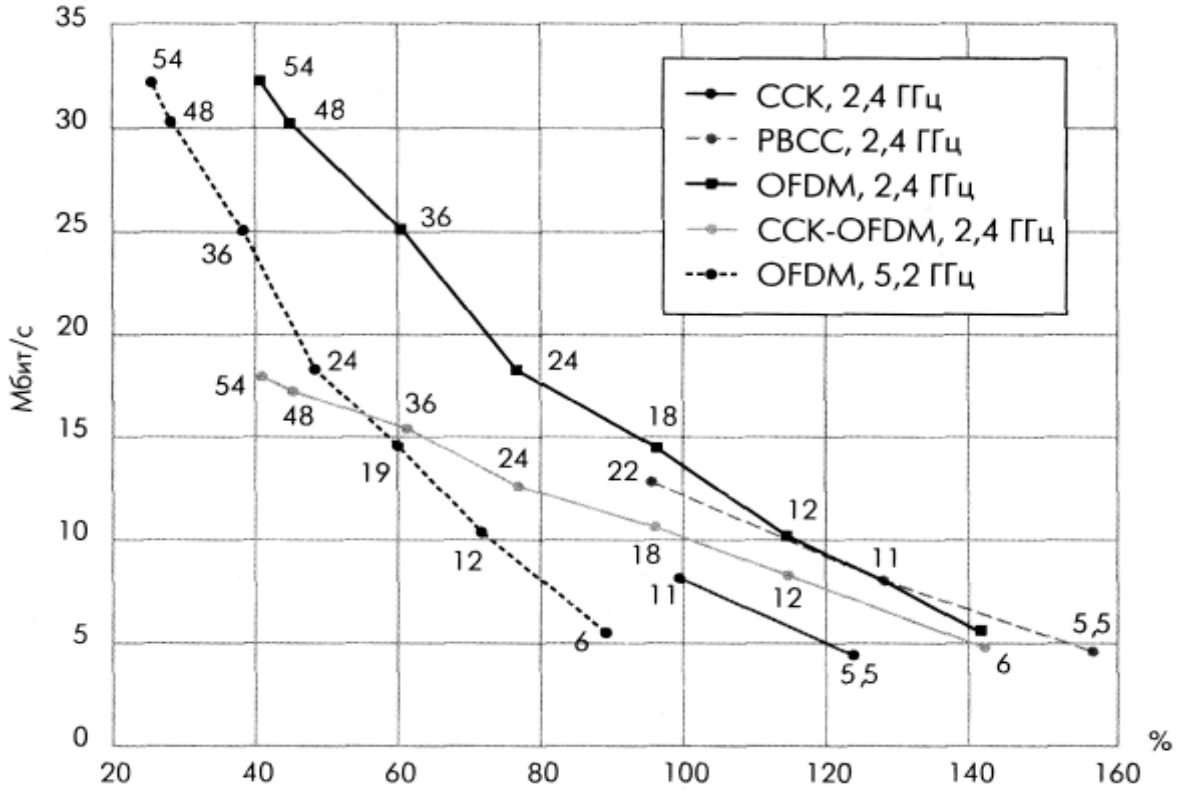


Рис. 7.57. Зависимость скорости передачи от расстояния для различных технологий передачи. Расстояние приведено в процентах, 100% - дальность передачи с модуляцией ССК на скорости 11 Мбит/с

Очевидно, что устройствам стандарта IEEE 802.11g достаточно долго придется работать в одних сетях с оборудованием 802.11b. Также очевидно, что производители в массе своей не будут поддерживать режимы CCK-OFDM и PBCC в силу их необязательности, ведь почти все решает цена устройства. Поэтому одна из основных проблем данного стандарта - как обеспечить бесконфликтную работу смешанных сетей 802.11b/g.

Основной принцип работы в сетях 802.11 - "слушать, прежде чем вещать". Но устройства 802.11b не способны услышать устройства802.11g в OFDM-режиме. Ситуация аналогична проблеме скрытых станций: два устройства удалены настолько, что не слышат друг друга и пытаются обратиться к третьему, которое находится в зоне слышимости обоих. Для предотвращения конфликтов в подобной ситуации в 802.11 введен защитный механизм, предусматривающий перед началом информационного обмена передачу короткого кадра "запрос на передачу" (RTS) и получение кадра подтверждения "можно передавать" (CTS). Механизм RTS/CTSприменим и к смешанным сетям 802.11b/g. Естественно, эти кадры должны транслироваться в режиме CCK, который обязаны понимать все устройства. Однако защитный механизм существенно снижает пропускную способность сети.

Таблица 7.10. Стандарты физического уровня

Параметр	802.11 DSSS	802.11 FHSS	802.11b	802.11a	802.11g
Частотный диапазон (ГГц)	2,4	2,4	2,4	5	2,4
Максимальная скорость передачи данных (Мбит/с)	2	2	11	54	54
Технология	DSSS	FHSS	CCK	OFDM	OFDM
Тип модуляции (для максимальной скорости передачи)	QPSK	GFSK	QPSK	64-QAM	64-QAM
Число неперекрывающихся каналов	3	3	3	15	3

Создание модели радиоинтерфейса WiFi 802.11 [21]

IEEE 802.11b

Чтобы открыть модель необходимо в командном окне ввести (Command Window): commwlan80211b. Появится модель, изображенная на рис.3.58.

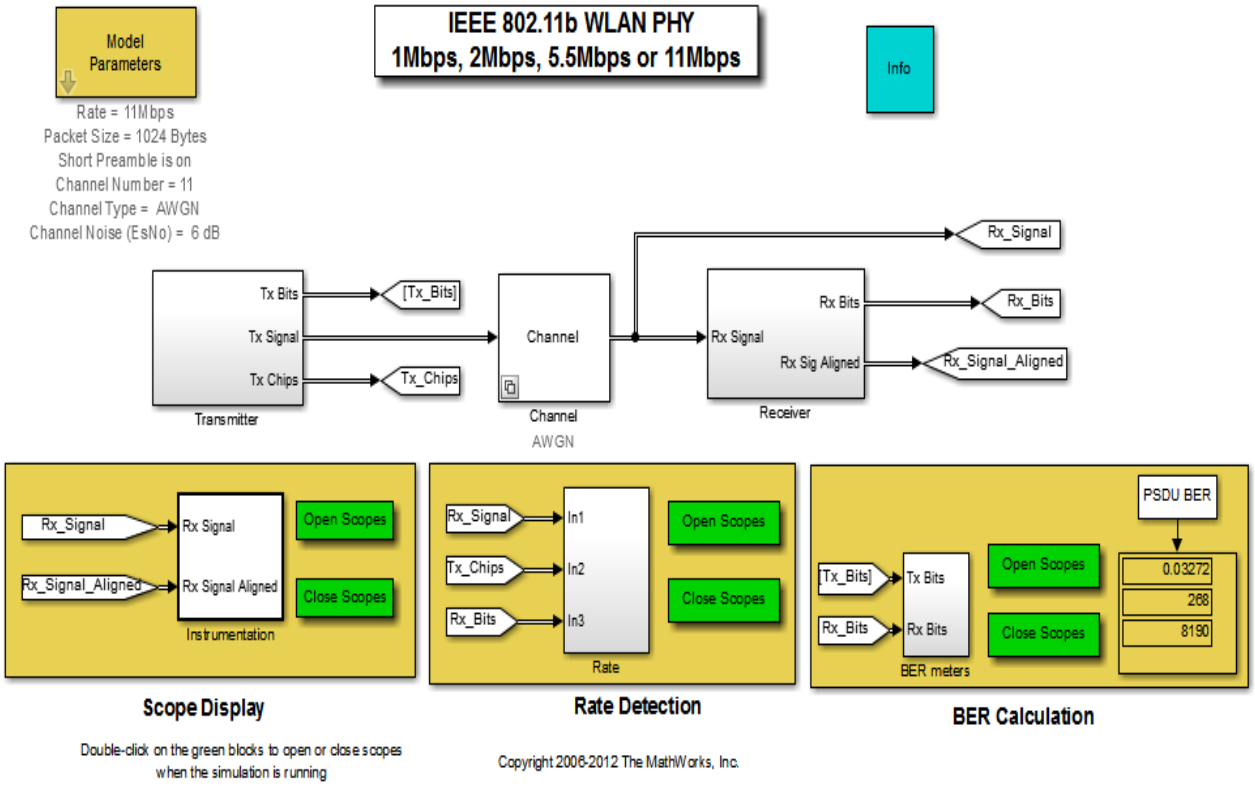


Рис. 7.58. Модель радиоинтерфейса 802.11b Simulink MATLAB 2015b

С помощью двойного щелчка на элемент Model Parameters можно устанавливать желаемые параметры моделируемой сети:

скорость передачи данных (Rate),

размер пакета (Packet Size),

число каналов (Channel Number),

тип канала (Channel Type),

уровень шумов в канале (Channel EsNo).

Двойным щелчком по передатчику, приемнику или каналу передачи можно посмотреть их структурные схемы. Они представлены на рис.7.59, рис.7.60, рис.7.61.

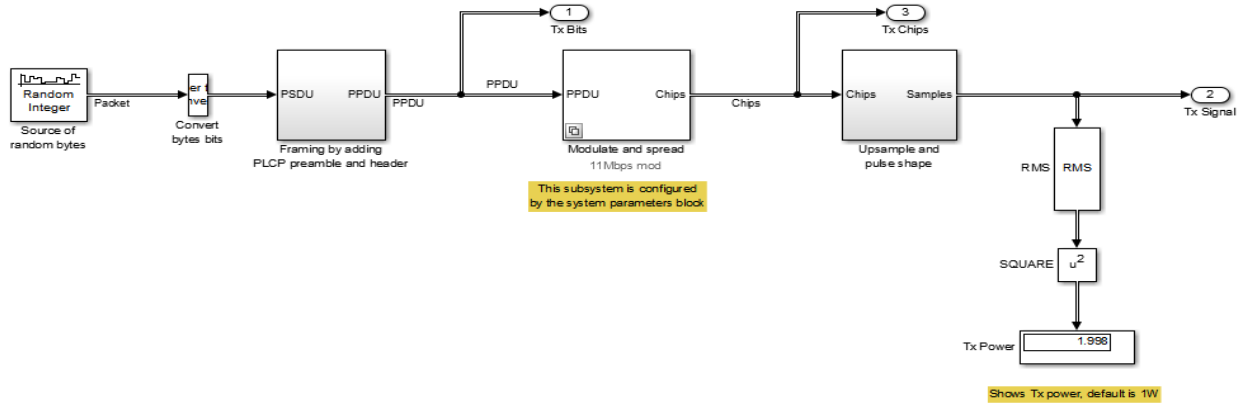


Рис. 7.59. Структурная схема передатчика IEEE 802.11b

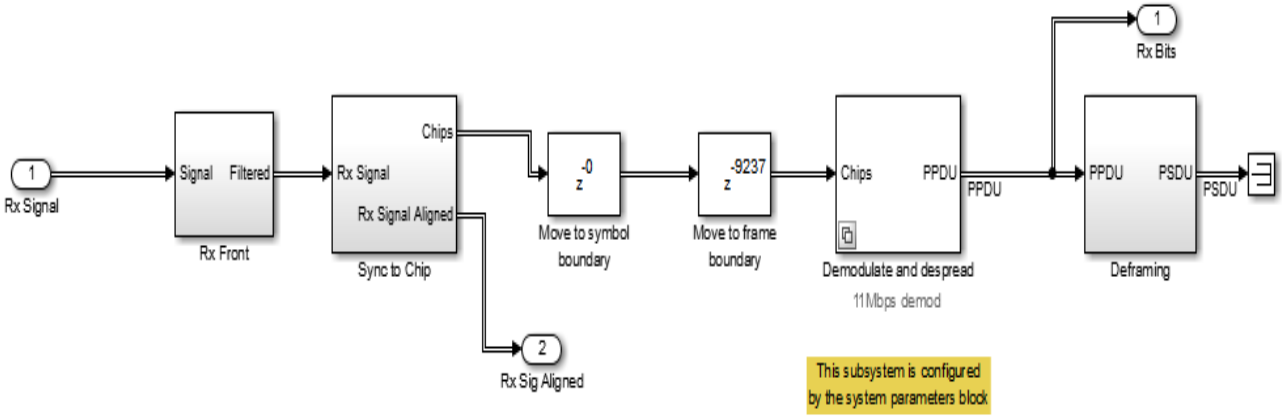


Рис. 7.60. Структурная схема приемника IEEE 802.11b

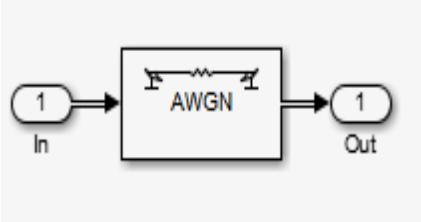


Рис. 7.61. Структурная схема канала передачи IEEE 802.11b

Пример частотной характеристика представлен на рис.7.62, а диаграмма созвездий на рис.7.63.

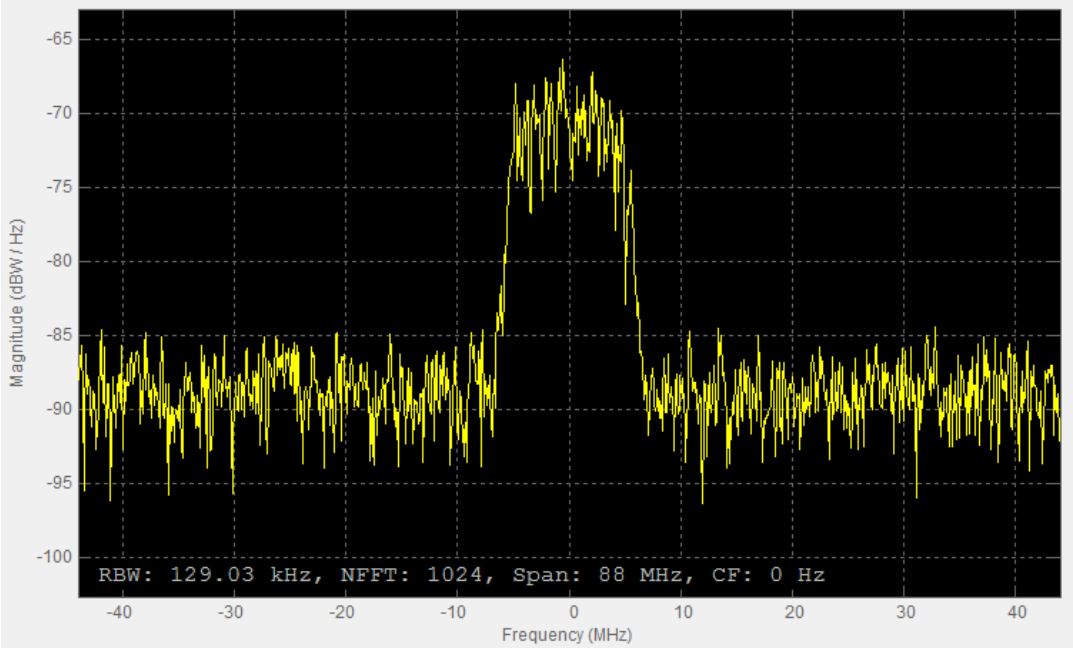


Рис. 7.62. Частотная характеристика для скорости передачи 11 Мбит/с

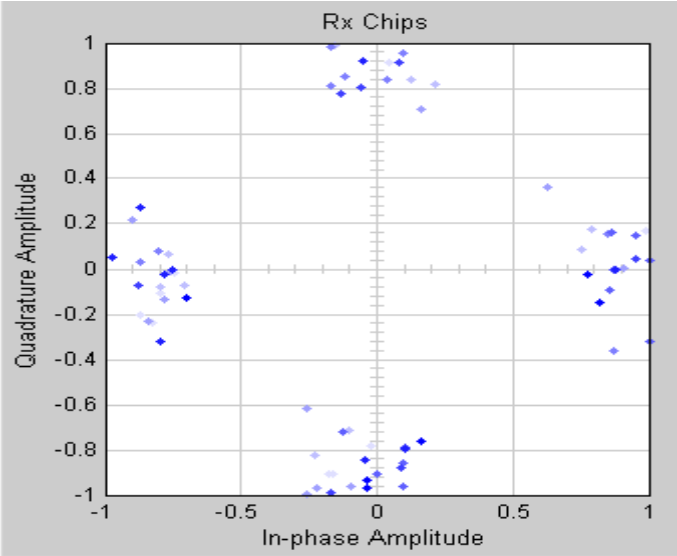


Рис. 7.63. Диаграмма созвездий для скорости передачи 11 Мбит/с

Исследование влияния ошибок BER

BitErrorRate (BER) - коэффициент ошибок, отношение числа неверно принятых битов (0 вместо 1 и наоборот) к полному числу переданных битов при передаче по каналу связи.

Чтобы получить зависимость BER от отношения сигнал/шум необходимо визменять уровень шумов в канале (0-14) и снимать показания в блоке BER Calculation в верхнем дисплее.

Протестировав систему таким образом, были получены зависимости, представленные на рис.7.64.

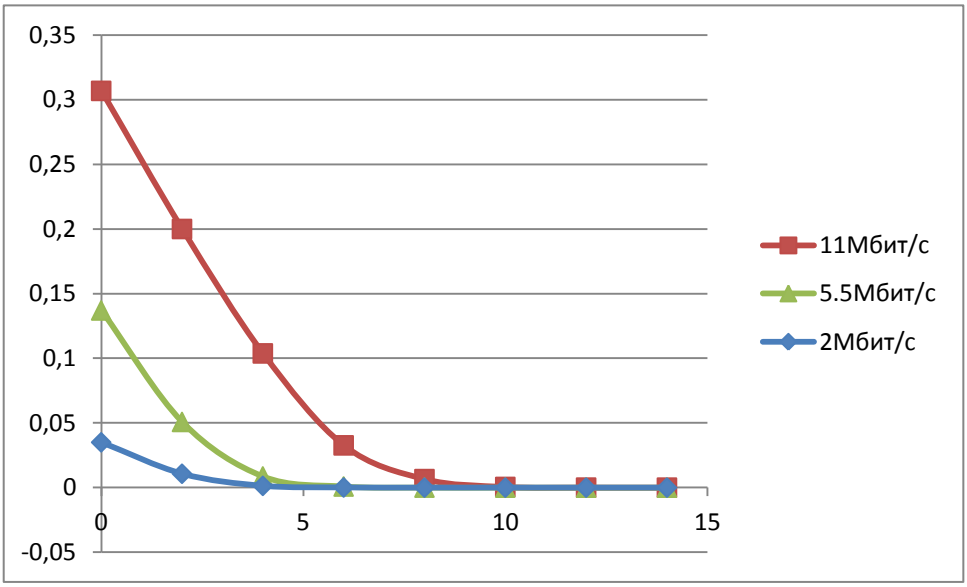


Рис. 7.64. Зависимость ошибки BER от отношения сигнал/шум для различных скоростей IEEE 802.11b

По полученным результатам можно сделать следующие выводы:

1) Большим скоростям соответствует большая вероятность появления ошибки

2) Для уменьшения ошибки необходимо увеличивать отношение сигнал/шум

3) Большим скоростям необходимо более высокое значение отношения сигнал шум для устранения возможных ошибок.

В результате работы изучены стандарты IEEE 802.11.

Рассмотрены и протестированы модели данных стандартов, реализованные в среде Simulink Matlab. Получены графики зависимостей вероятности ошибки (BER) от отношения сигнал/шум для разных скоростей.

Методические указания к моделированию

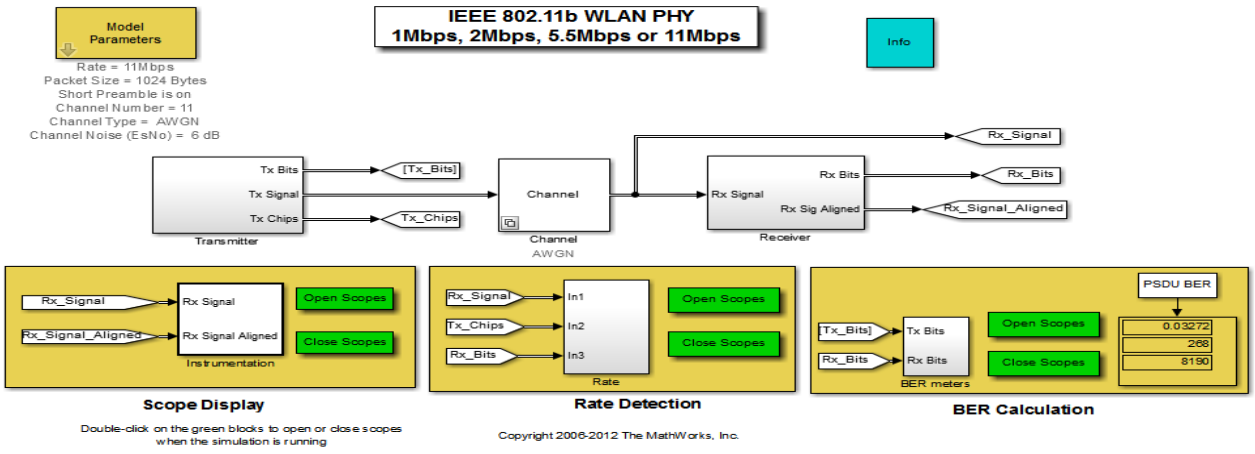


Рис. 7.65. Схем сети IEEE 802.11b MATLAB

1. Запустить модель командой commwlan80211b и изучить ее параметры. Сделать скриншоты полной схемы, а также передатчика, приёмника и канала.

2. Снять частотную характеристику, а также диаграмму созвездий для 4-х вариантов максимальной скорости передачи (1, 2, 5, 11 Мбит/с). Параметр «тип канала» (Channel Type) – none.

3. Для каждой скорости изменяя отношение сигнал/шум в канале от 0 до 14дБ снять зависимость BER от Channel EsNo. Параметр «тип канала» (Channel Type) – AWGN.

5. Сделать выводы по проделанной работе.

7.4. Имитационное моделирование системы мобильной связи стандарта IEEE 802.15.4 ZigBee

Среди наиболее известных беспроводных технологий можно выделить: Wi-Fi, Wi-Max, Bluetooth, Wireless USB и относительно новую технологию — ZigBee, которая изначально разрабатывалась с ориентацией на промышленные применения.

Каждая из этих технологий имеет свои уникальные характеристики, которые определяют соответствующие области применения.

Стандарт	802.15.4 ZigBee™			802.15.1 Bluetooth	802.15.3 High Rate WPAN, WiMedia	802.15.3a* UWB	802.11b Wi-Fi
Приложения	Мониторинг, управление, сети датчиков, домашняя/промышленная автоматика			Голос, данные, замена кабелей	Потоковое мультимедиа, замена кабелей аудио/видеосистем		Данные, видео, ЛВС
Преимущества	Цена, энергосбережение, размеры сети, менее загруженные диапазоны		Цена, энерго-сбережение, размеры сети, глобальный диапазон	Цена, энерго-сбережение, передача голоса, перескоки частоты	Высокая скорость, энергосбережение		Скорость, гибкость
Частота, ГГц	0,868	0,915	2,4			3,1 – 10,6	2,4
Макс. скорость	20 Кбит/с	40 Кбит/с	250 Кбит/с	1 Мбит/с	22 Мбит/с (доп. 11, 33, 44, 55 Мбит/с)	110 Мбит/с (10 м), 200 Мбит/с (4 м) (доп. 480 Мбит/с)	11 Мбит/с
Выходная мощность (ном.), дБм	0			0 (класс 3) 4 (класс 2) 20 (класс 1)	0	< 20 (110 Мбит/с) < 24 (200 Мбит/с)	20
Дальность, м	10 – 100			10 (класс 3) 100 (класс 1)	5 – 50	10 (110 Мбит/с) 4 (200 Мбит/с)	100
Чувствительность (спецификация, дБм)	-92		-85	-70	-75	-	-76
Размер стека, Кбайт	4 – 32			> 250	-		> 1000
Срок службы батареи, дней	100 – 1000+			1 – 7	теоретически более 1000		0,5 – 5
Размер сети	65536 (16-битные адреса), 2^{64} (64-битные адреса)			мастер +7	до 127 на хост		32

Рис. 7.66. Основные характеристики популярных стандартов беспроводной связи

Рис. 7.67. Внешний вид микросхемы ZigBee

Анализ беспроводных технологий показывает, что высокоскоростные технологии Wi-Fi, Wi-Max, Bluetooth, Wireless USB предназначены в первую очередь для обслуживания компьютерной периферии и устройств мультимедиа. Они оптимизированы для передачи больших объемов информации на высоких скоростях, работают в основном по топологии «точка-точка» или «звезда» и малопригодны для реализации сложных разветвленных промышленных сетей с большим количеством узлов. Напротив, технология ZigBee имеет достаточно скромные показатели скорости передачи данных и расстояния между узлами, но обладает следующими важными, с точки зрения применения в промышленности, преимуществами:

Она ориентирована на преимущественное использование в системах распределенного мульти-микропроцессорного управления со сбором информации с интеллектуальных датчиков, где вопросы минимизации энергопотребления и процессорных ресурсов являются определяющими.

Предоставляет возможность организации самоконфигурируемых сетей со сложной топологией, в которых маршрут сообщения автоматически определяется не только числом исправных или включенных/выключенных на текущий момент устройств (узлов), но и качеством связи между ними, которое автоматически определяется на аппаратном уровне.

Обеспечивает масштабируемость — автоматический ввод в работу узла или группы узлов сразу после подачи питания на узел.

Гарантирует высокую надежность сети за счет выбора альтернативного маршрута передачи сообщений при отключениях/сбоях в отдельных узлах.

Поддерживает встроенные аппаратные механизмы шифрации сообщений AES-128, исключая возможность несанкционированного доступа в сеть.

Организация сети ZigBee

ZigBee — относительно новый стандарт беспроводной связи, который изначально разрабатывался как средство для передачи небольших объемов информации на малые расстояния с минимальным энергопотреблением. Фактически этот стандарт описывает правила работы программно-аппаратного комплекса, реализующего беспроводное взаимодействие устройств друг с другом.

Стек протоколов ZigBee представляет собой иерархическую модель, построенную по принципу семиуровневой модели протоколов передачи данных в открытых системах OSI (OpenSystemInterconnection). Стек включает в себя уровни стандарта IEEE 802.15.4, отвечающие за реализацию канала связи, и программные сетевые уровни и уровни поддержки приложений, определенные спецификацией ZigBee. Модель реализации стандарта связи ZigBee представлена на рисунке 7.69.

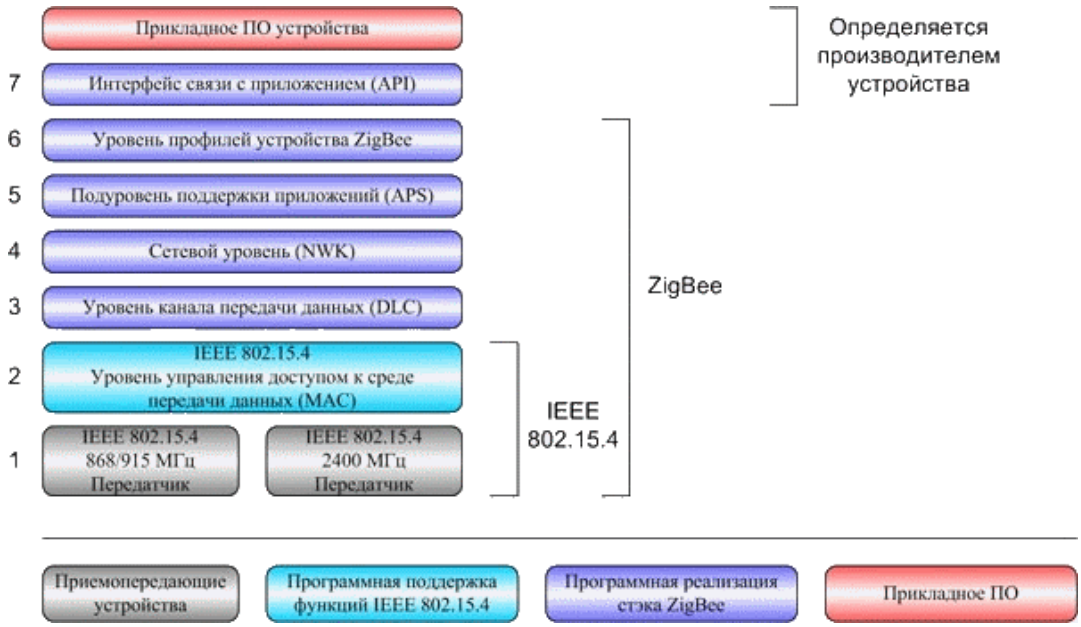


Рис. 7.68. Многоуровневая модель стандарта связи ZigBee

Стандарт IEEE 802.15.4 определяет два нижних уровня стека: уровень доступа к среде (MAC) и физический уровень передачи данных в среде распространения (PHY), то есть нижние уровни протокола беспроводной передачи данных. Альянс определяет программные уровни стека ZigBee от уровня канала передачи данных (DataLinkControl) до уровня профилей устройств (ZigBeeProfiles). Прием и передача данных по радиоканалу осуществляется на физическом уровне PHY, определяющем рабочий частотный диапазон, тип модуляции, максимальную скорость, число каналов. Уровень PHY осуществляет активацию-дезактивацию приемопередатчика, детектирование энергии принимаемого сигнала на рабочем канале, выбор физического частотного канала, индикацию качества связи при получении пакета данных и оценку свободного канала. Важно понимать, что стандарт 802.15.4 — это физическое радио (микросхема радио-приемопередатчика), а ZigBee — это логическая сеть и программный стек, обеспечивающие функции безопасности и маршрутизации.

Далее в структуре стека ZigBee следует уровень контроля доступа к среде IEEE 802.15.4 MAC, осуществляющий вход и выход из сети устройств, организацию сети, формирование

пакетов данных, реализацию различных режимов безопасности (включая 128-битное шифрование AES), 16- и 64-битную адресацию.

Уровень MAC обеспечивает различные механизмы доступа в сеть, поддержку сетевых топологий от «точка-точка» до «многоячейковая сеть», гарантированный обмен данными (ACK, CRC), поддерживает потоковую и пакетную передачи данных.

Для предотвращения нежелательных взаимодействий возможно использование временного разделения на основе протокола CSMA-CA (протокол множественного доступа к среде с контролем несущей и предотвращением коллизий).

Временное разделение ZigBee базируется на использовании режима синхронизации, при котором подчиненные сетевые устройства, большую часть времени находящиеся в «спящем» состоянии, периодически «просыпаются» для приема сигнала синхронизации от сетевого координатора, что позволяет устройствам внутри локальной сетевой ячейки знать, в какой момент времени осуществлять передачу данных. Данный механизм, основанный на определении состояния канала связи перед началом передачи, позволяет существенно сократить (но не устранить) столкновения, вызванные передачей данных одновременно несколькими устройствами. Стандарт 802.15.4 основывается на полудуплексной передаче данных (устройство может либо передавать, либо принимать данные), что не позволяет использовать метод CSMA-CA для обнаружения коллизий — только для их предотвращения.

В спецификации стека предусмотрены три типа устройств: координатор, маршрутизатор и конечное устройство.

Координатор инициализирует сеть, управляет ее узлами, хранит информацию о настройках каждого узла, задает номер частотного канала и идентификатор сети PAN ID, а в процессе работы может являться источником, приемником и ретранслятором сообщений.

Маршрутизатор отвечает за выбор пути доставки сообщения, передаваемого по сети от одного узла к другому, и в процессе работы также может являться источником, приемником или ретранслятором сообщений. Если маршрутизаторы имеют соответствующие возможности, они могут определять оптимизированные маршруты к определенной точке и хранить их для последующего использования в таблицах маршрутизации.

Оконечное устройство не участвует в управлении сетью и ретрансляции сообщений, являясь только источником/приемником сообщений.

Среди свойств ZigBee следует особо выделить поддержку сложных топологий сетей. Именно за счет этого, при относительно малой максимальной дальности связи двух близлежащих устройств, возможно расширить зону покрытия сети в целом. Также этому способствует 16-битная адресация, позволяющая объединять в одну сеть более 65 тыс. устройств.

Спецификация стандарта IEEE 802.15.4

Спецификация ZigBee-стека определяет сетевой уровень, уровни безопасности и доступа к приложению и может использоваться совместно с решениями на базе стандарта 802.15.4 для обеспечения совместимости устройств.

Таблица 7.11. Спецификация стандарта IEEE 802.15.4

Стандарт	802.15.4 ZigBee™		
Частота	868 МГц	915 МГц	2,4 ГГц
Число каналов/шаг	1/–	10/2 МГц	16/5 МГц
География распространения	Европа	Америка	Весь мир
Макс. скорость, модуляция	20 кбит/с, BPSK	40 кбит/с, BPSK	250 кбит/с, O-QPSK
Выходная мошность, ном.	0 dBm (1 мВт)	0 dBm (1 мВт)	0 dBm (1 мВт)
Дальность	10–100м		
Чувствительность (спецификация)	–92dBm	–92dBm	–85dBm
Размер стека	4–32 кбайт		
Срок службы батареи	От 100 до 1000 и более дней		
Размер сети	65536 (16-битные адреса), 264 (64-битные адреса)		

Практическая часть

Задание:

Собрать схему

Подготовить схемы для реализации Стандарта ZigBee 802.15.4 основываясь на примере, представленном в отчете.

Изменять SNR в пределах от 1 до 100 (не менее 4-х точек)

Построить графики зависимости SNR от BER

Все поэтапное исследование представить в отчете.

В рабочем поле необходимо собрать схему для работы стандарта ZigBee 802.15.4. Схема представлена на рисунке 3.70.

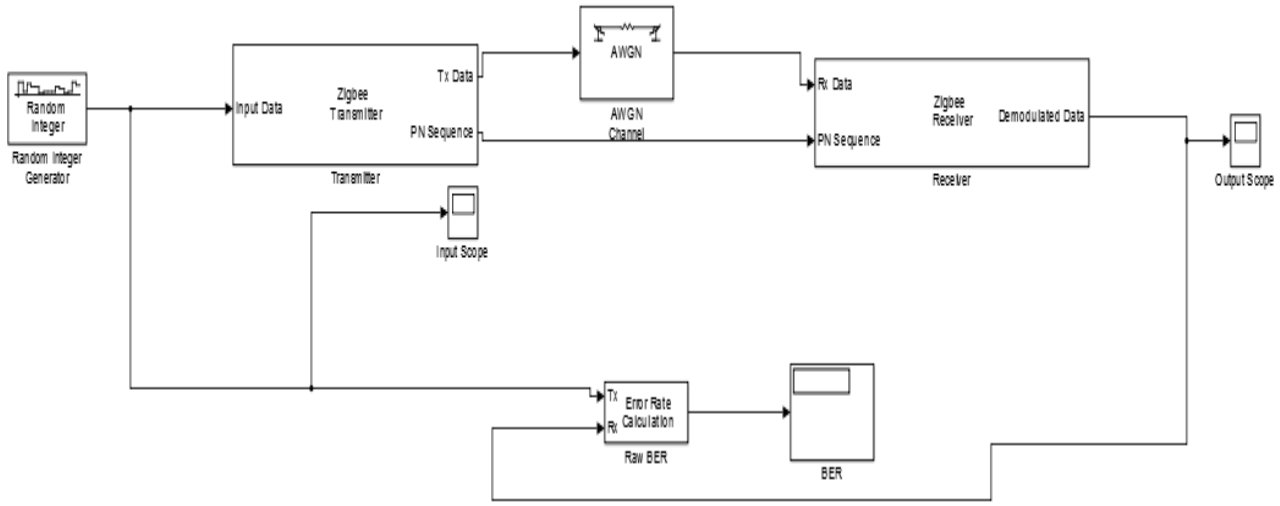


Рис. 7.69. Схема стандарта ZigBee 802.15.4 Simulink MATLAB 2015b

В состав схемы входят:

RandomIntegerGenerator

ZigBeeTransmitter

AWGN Channel (каналпередачи)

ZigBeeReciever

ErrorRateCalculation (анализаторошибок)

Display

Рассмотрим каждый блок отдельно. Все значения, заданные в блоках, помимо отношения Сигнал/шум в канале, остаются неизменными.

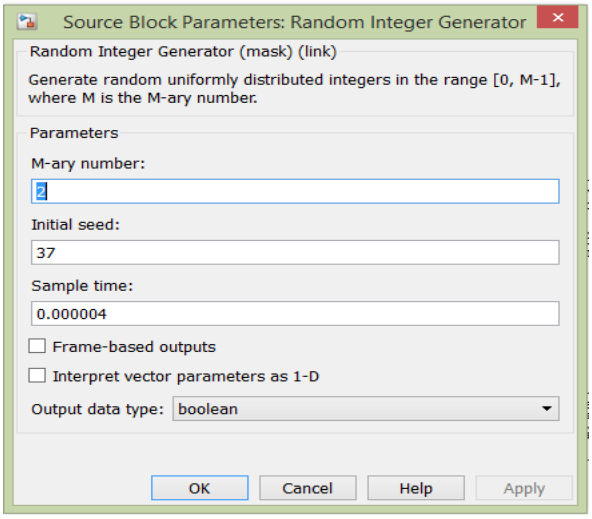


Рис. 7.70. Параметры блока Random Integer Generator

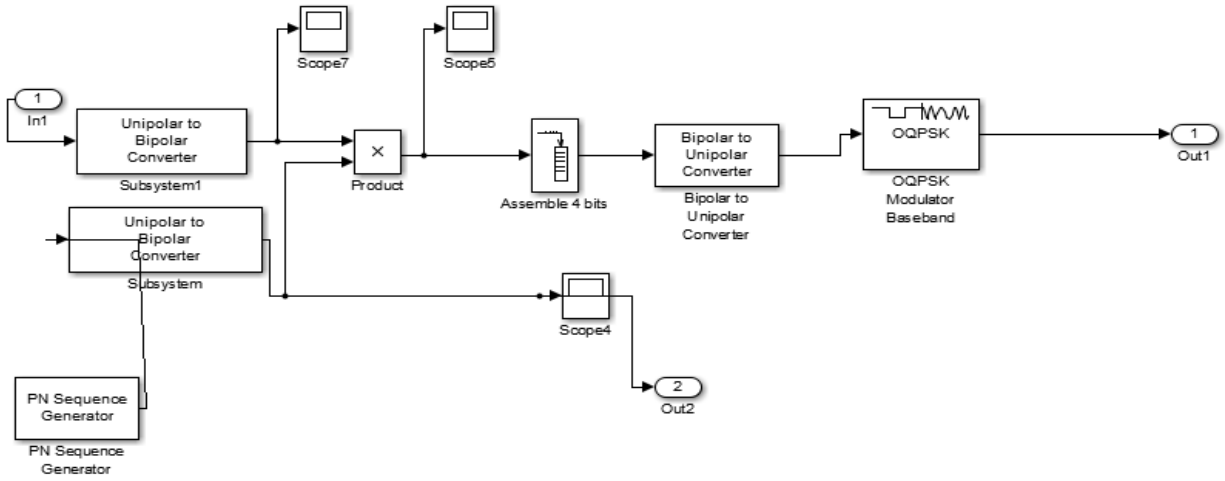


Рис. 7.71. Схема ZigBeeTransmitter

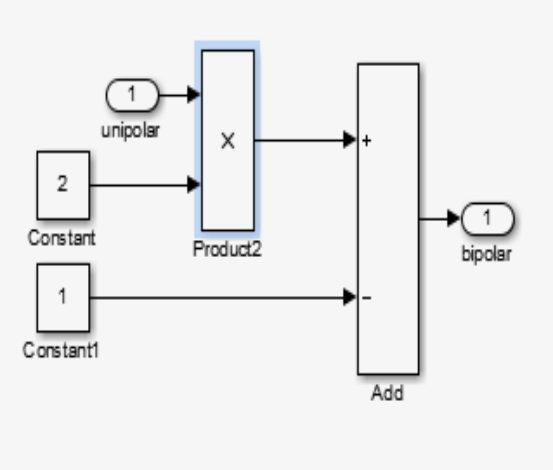


Рис. 7.72. Unipolar to bipolar converter

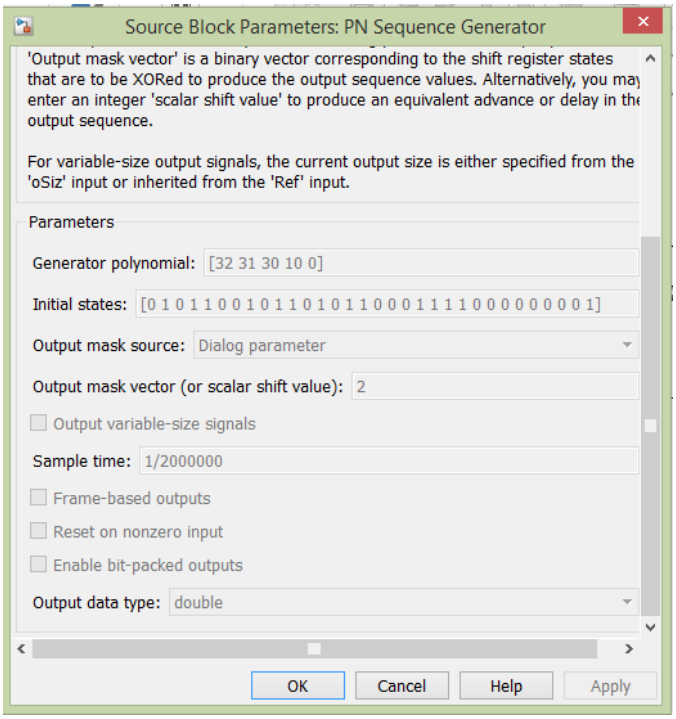


Рис. 7.73. Параметры блока PN sequence generator

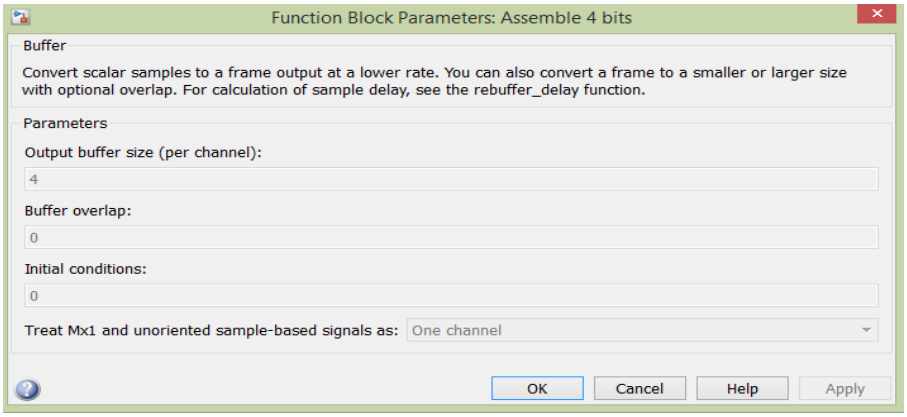


Рис. 7.74. Параметры блока Function block parameters: Assemble 4 bits

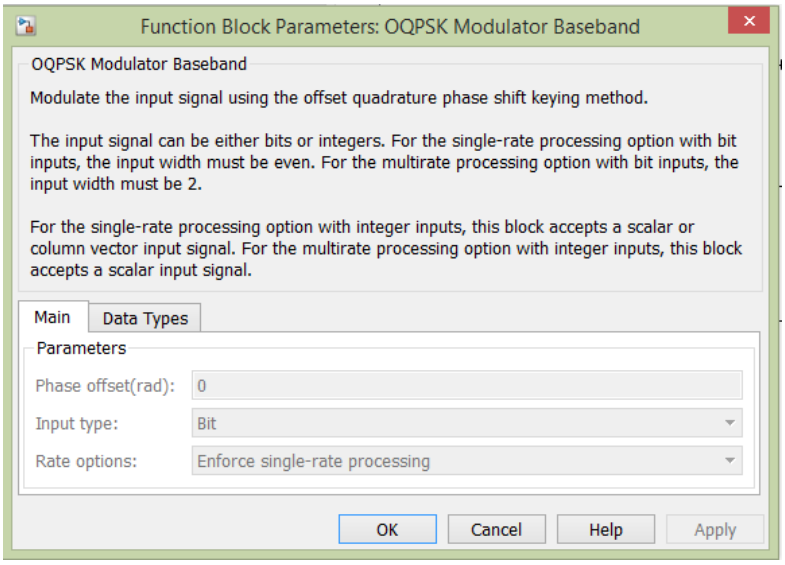


Рис. 7.75. Параметры блока OQPSK modulator baseband

OQPSK - четырехпозиционная фазовая модуляции со сдвигом квадратур (OQPSK), где битовые потоки, подаваемые на модуляторы квадратур I и Q, сдвинуты друг относительно друга на длительность одного бита (половина символьного интервала).

Рассмотрим блок канала с БГШ. В данном блоке необходимо изменять значения в строчке Eb\No от 1 до 100.

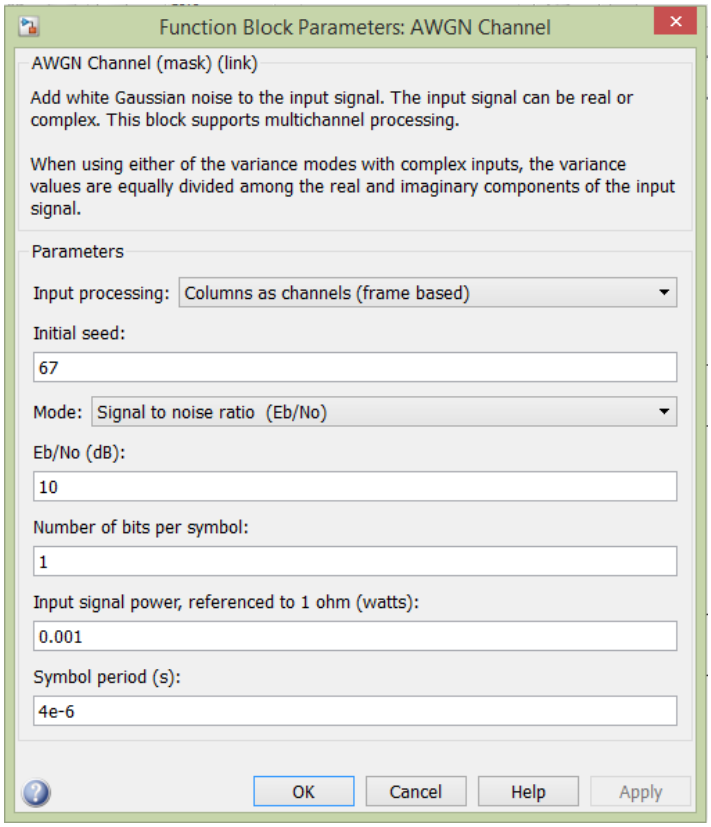


Рис. 7.76. Параметры блока AWGNchannel

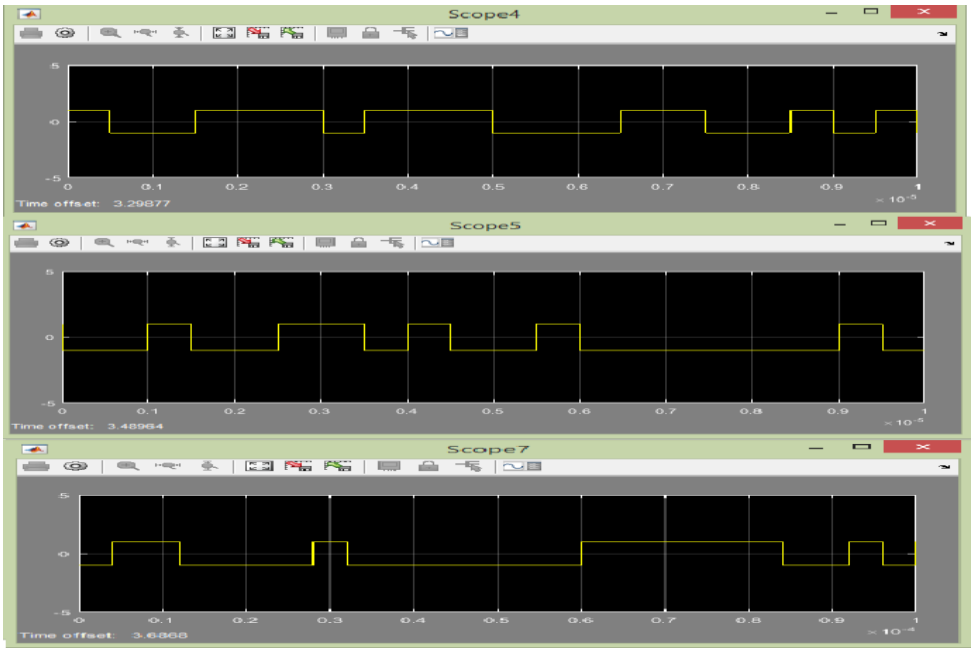


Рис. 7.77. Вид сигнала на осциллографах 4, 5, 7

Рассмотрим подробнее блок ZigBee Receiver.

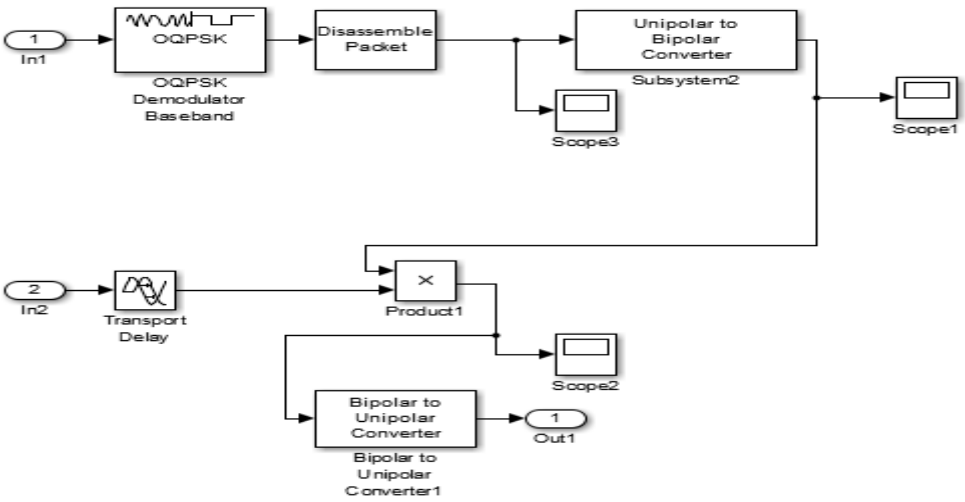


Рис. 7.78. Схема приемника стандарта ZigBee

Рассмотрим каждый блок отдельно. Единственным незнакомым элементом является блок TransportDelay.

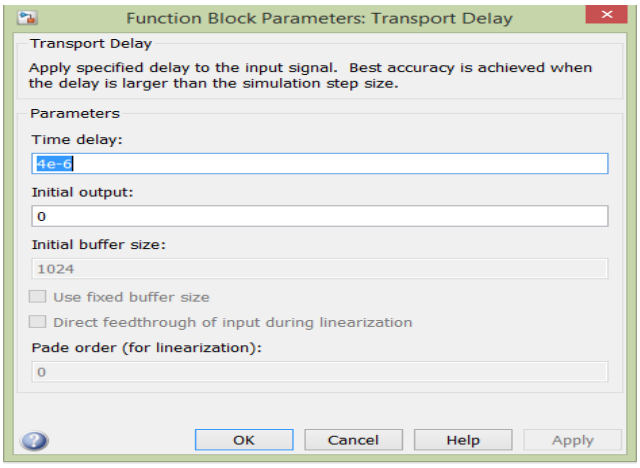


Рис. 7.79. Параметры блока TransportDelay

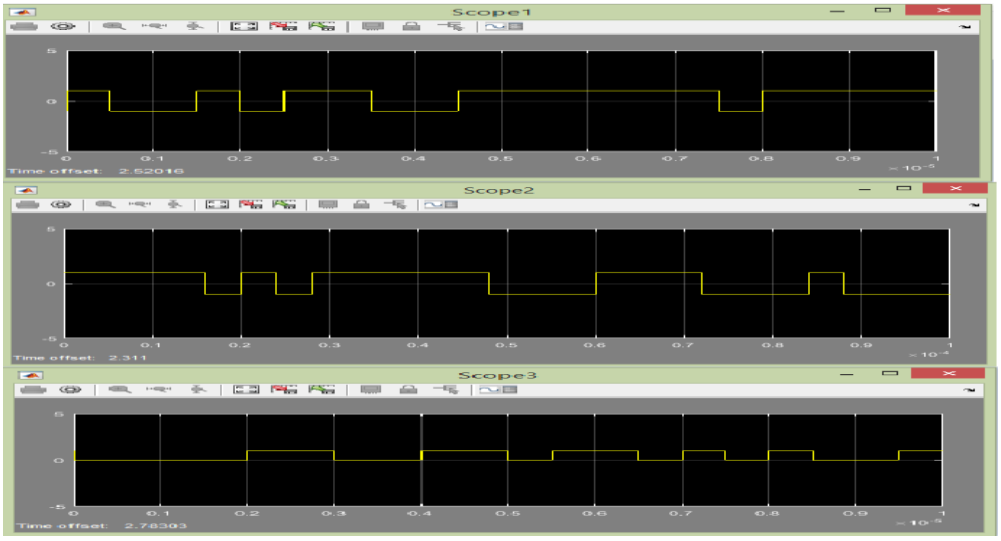


Рис. 7.80. Вид сигнала на осциллографах 1, 2, 3

Вернемся к общей схеме стандарта ZigBee.

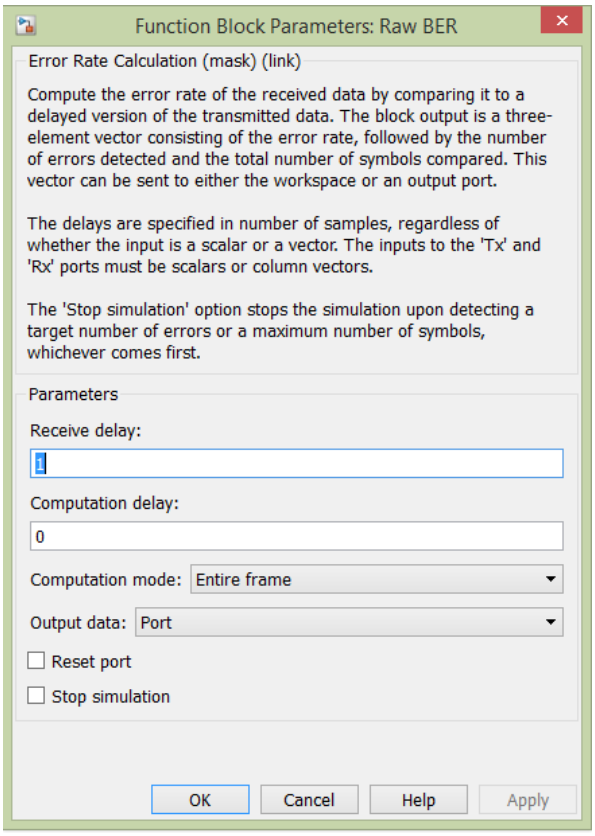


Рис. 7.81. Параметры блока RawBER

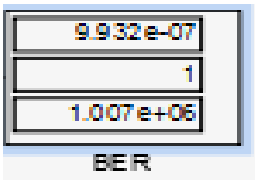


Рис. 7.82. Счетчик ошибок

Для построения графика зависимости BER от SNR, необходимо из счетчика брать первую строку.

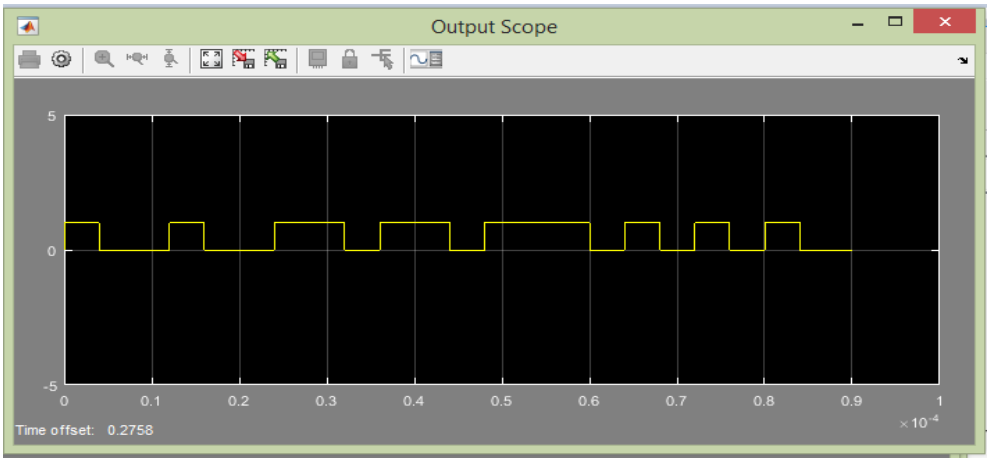


Рис. 7.83. Вид сигнала на выходе

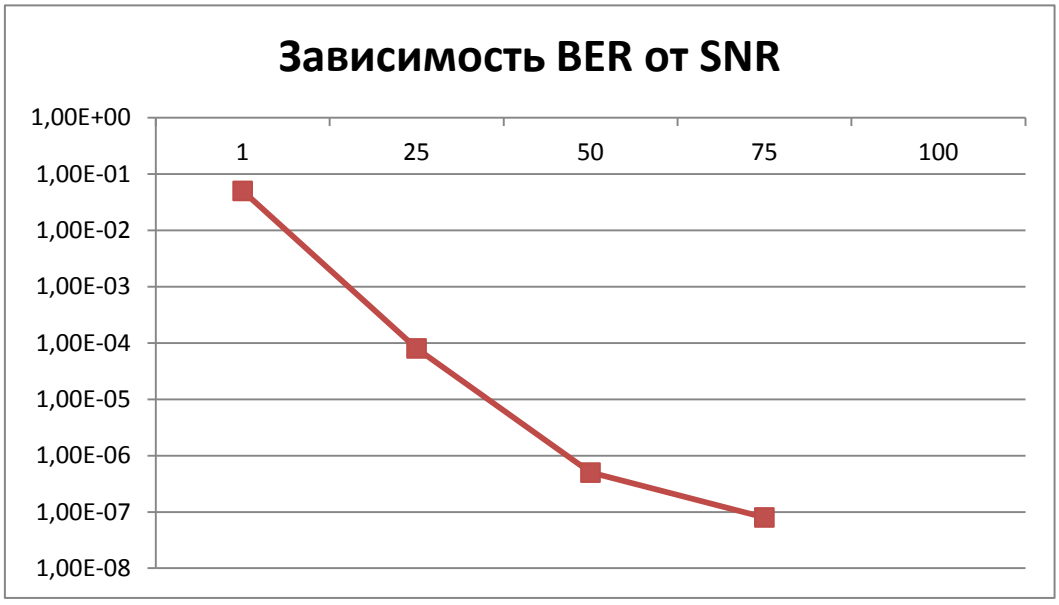


Рис. 7.84. График зависимости BER от SNR

В разделе построена схема стандарта ZigBee 802.15.4 в среде Simulink. Построен график зависимостей зависимости BER от SNR. Из графика (рисунок 5.85) видно, что при увеличении значения сигнал/шум, снижается количество ошибок.

7.5. Проектирование защищенной системы мобильной связи стандарта IEEE 802.15.1 (Bluetooth)

Bluetooth

Стандарт Bluetooth является компромиссным с точки зрения соотношения параметров экономичность/дальность/скорость. По своей функциональности и возможности применения в различных приложениях он имеет наибольшее число пересечений с другими стандартами группы Short Range RF. Поэтому для начала рассмотрим именно его.

Основная идея Bluetooth заключалась в создании универсального, надежного и очень дешевого радиоинтерфейса беспроводного доступа. Технология Bluetooth позволяет обеспечить сопряжение с различным профессиональным и бытовым оборудованием в режимах передачи речи, данных и мультимедиа, при этом гарантируется его электромагнитная совместимость с другим домашним или офисным оборудованием. Как было указано в таблице, существует всего три класса устройств Bluetooth, если градировать их по излучаемой мощности: 1-й — до 100 метров (до 100 мВт); 2-й — до 10 метров (до 2,5 мВт); 3-й — до 1 метра (до 1 мВт).

Для определения модели поведения при установлении соединения между различными типами устройств в технологии Bluetooth введено понятие профиль. Этим термином

обозначается набор функций и возможностей, которые использует Bluetooth в качестве механизма транспортировки. Профили гарантируют возможность обмена информацией между устройствами разных производителей. Bluetooth SIG определяет 15 стандартных профилей:

Generic Access Profile (GAP);

Service Discover Application Profile (SDAP);

Serial Port Profile (SPP);

Dial-up Networking Profile (DUNP);

Generic Object Exchange Profile (GOEP);

Object Push Profile (OPP);

File Transfer Profile (FTP);

Synchronization Profile (SP);

AV Control, Headset Profile (HSP);

Advanced Audio Distribution Profile (A2DP);

Basic Imaging Profile (BIP);

Handsfree Profile (HFP);

Human Interface Device Profile (HID);

LAN Access Profile (LAP);

Sim-Card Access Profile (SAP).

По характеру взаимодействия со внешними устройствами и приложениями архитектура всех существующих модулей Bluetooth может быть разделена на три вида (рис. 1). Модули с двухпроцессорной архитектурой (рис. 1а) не содержат в себе программного высокоуровневого стека Bluetooth с поддержкой стандартных профилей. Это значит, что необходимые профили Bluetooth должны быть реализованы на внешнем процессоре. Взаимодействие внешнего процессора с модулем происходит через виртуальный интерфейс HCI (Host Controller Interface). В частном случае HCI может быть реализован через аппаратный интерфейс SPI или UART.

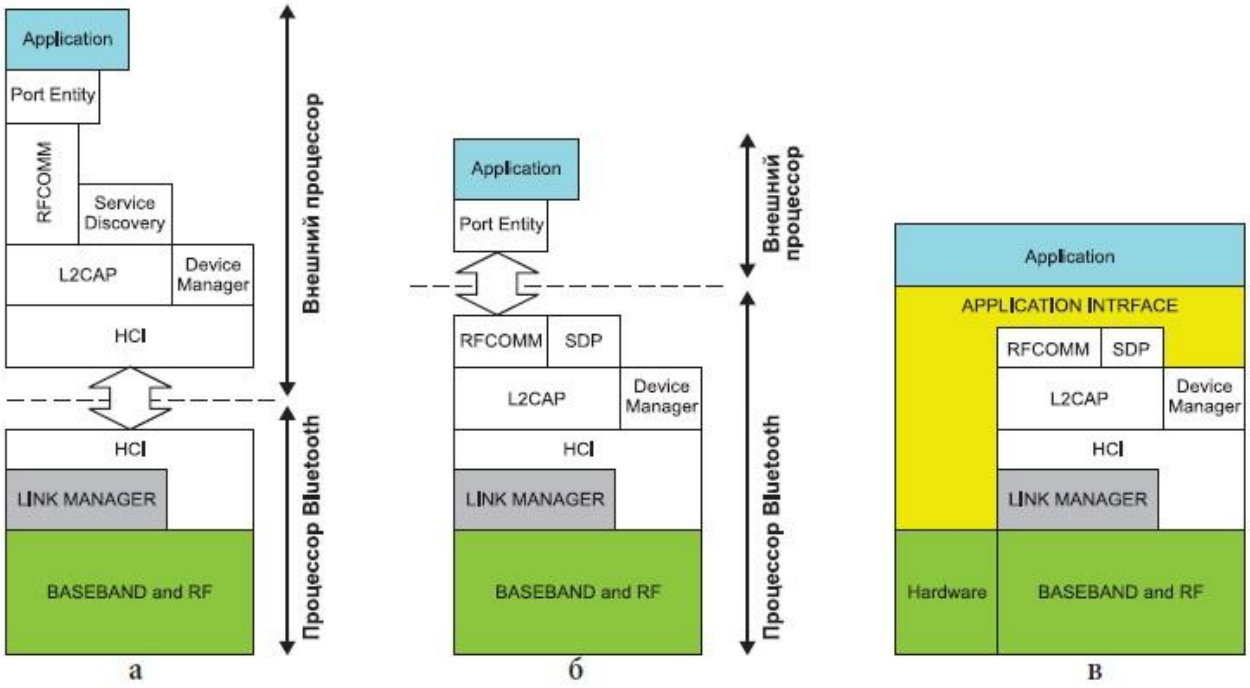


Рис. 7.85. Разновидности архитектуры модулей стандарта Bluetooth: а) двухпроцессорная; б) встроенная двухпроцессорная; в) однопроцессорная

Модули Bluetooth со встроенной двухпроцессорной архитектурой (рис. 3.85б) являются наиболее распространенными. Данная разновидность архитектуры подразумевает наличие стека Bluetooth высокого уровня с поддержкой стандартных профилей непосредственно во внутреннем процессоре модуля. В этом случае приложение, работающее на внешнем процессоре, взаимодействует с модулем Bluetooth через аппаратные интерфейсы.

Однопроцессорная архитектура (рис. 3.85в) является наименее распространенной. Для ее реализации разработчик должен создать специальное приложение, которое будет работать на внутреннем процессоре модуля Bluetooth. В этом случае модуль превращается в автономное устройство, доступ к которому через внешние аппаратные интерфейсы закрыт.

Принадлежность модуля к той или иной архитектуре может определяться как его аппаратной реализацией, так и внутренним программным обеспечением. Например, в частном случае один и тот же модуль Bluetooth может быть отнесен к любой из трех разновидностей архитектуры в зависимости от типа прошивки, загруженной во внутренний процессор модуля. Такой подход пользуется наибольшей популярностью среди зарубежных производителей.

Чтобы получить наиболее полное представление о роли Bluetooth среди других представителей группы Short Range RF, обратимся к истории (рис. 5.86). Развитие Bluetooth с самого начала шло по пути увеличения скорости обмена данными, снижения

энергопотребления, повышения безопасности и надежности соединения. Вплоть до версии 3.0 сохранялась обратная совместимость всех версий Bluetooth между собой. До сих пор в эксплуатации встречаются устройства Bluetooth версий 1.1 и 1.2, которые успешно используются совместно с 2.0 и 2.1.

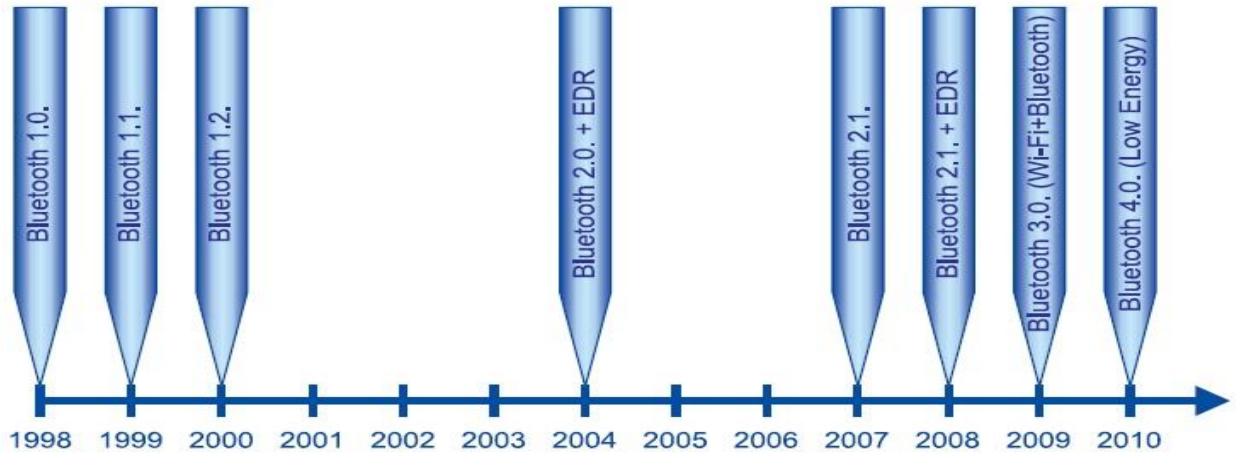


Рис. 7.86. Хронология развития стандарта Bluetooth

Bluetooth 3.0 является чем-то средним между Bluetooth и Wi-Fi. Модули с ее поддержкой соединяют в себе две радиосистемы: первая обеспечивает передачу данных в 3 Мбит/с (стандартная для Bluetooth 2.0) и имеет низкое энергопотребление; вторая совместима со стандартом 802.11 (Wi-Fi) и обеспечивает возможность передачи данных со скоростью до 24 Мбит/с (сравнима со скоростью сетей Wi-Fi). Выбор радиосистемы для передачи данных зависит от размера передаваемого файла. Это один из наиболее ярких примеров объединения двух разных технологий для завоевания новых сегментов рынка. Правда, успеха эта попытка не имела: распространения Bluetooth 3.0 не получил.

Bluetooth 4.0 не имеет обратной совместимости с предыдущими версиями. Сверхнизкое энергопотребление достигается за счет использования специального алгоритма работы. Передатчик включается только на время отправки данных, что обеспечивает возможность работы от одной батарейки типа CR2032 в течение нескольких лет. Стандарт предоставляет скорость передачи данных в 1 Мбит/с при размере пакета 8–27 байт. В новой версии два Bluetooth-устройства смогут устанавливать соединение менее чем за 5 мс и поддерживать его на расстоянии до 100 м. Для этого используется усовершенствованная коррекция ошибок, а необходимый уровень безопасности обеспечивает 128-битное шифрование.

Предполагается, что Bluetooth 4.0 будет конкурировать и вытеснять ZigBee в классе малопотребляющих радиочастотных устройств с поддержкой сложных сетей. Это также является ярким примером пересечения двух разных технологий, в данном случае — ZigBee и Bluetooth.

Проанализировав современное состояние технологии Bluetooth, можно обозначить плюсы и минусы. К достоинствам стандарта относятся:

высокий уровень стандартизации и совместимость между устройствами Bluetooth разных производителей;

защита передаваемых данных;

низкая стоимость;

высокая дальность действия (до 1000 м);

универсальность и большое разнообразие модулей под разные задачи.

Среди недостатков отметим:

Относительно высокое энергопотребление (работа от автономных источников питания не всегда возможна). Предполагается, что этого недостатка будет лишена новая версия спецификации Bluetooth 4.0.

Относительно невысокая скорость обмена данными (до 1 Мбит/с). Как правило, реальная скорость обмена данными ограничивается пропускной способностью внешних аппаратных интерфейсов модуля.

Одно из основных преимуществ стандарта Bluetooth заключается в его высоком уровне стандартизации и широчайшем распространении в составе пользовательских электронных устройств. Это позволяет в ряде случаев практически в два раза сэкономить время и затраты на разработку при проектировании некоторой системы сбора данных, телеметрии или управления на основе Bluetooth, поскольку в качестве одной из сторон беспроводного обмена данными может выступать, например, обычный серийно выпускаемый ноутбук или коммуникатор с поддержкой данной технологии.

Исходя из характерных особенностей модулей Bluetooth, сформировались их области применения в России и за рубежом:

Автомобильная электроника. Модули Bluetooth могут использоваться в бортовых автомобильных системах контроля и управления. Эта область применения характерна для России.

Системы удаленного управления и телеметрии. Здесь устройства Bluetooth могут использоваться наряду с модулями технологий Wi-Fi, ZigBee, Short Range RF 434/868 МГц. Данная область применения в равной степени актуальна как для России, так и для зарубежных стран.

Bluetooth

Ноутбуки, сотовые телефоны, смартфоны, торговые терминалы со встроенной функцией Bluetooth. Bluetooth - это современная технология беспроводной передачи данных, позволяющая соединять друг с другом практически любые устройства: мобильные

телефоны, ноутбуки, принтеры, цифровые фотоаппараты и даже холодильники, микроволновые печи, кондиционеры. Соединить можно все, что соединяется (то есть имеет встроенный микрочип Bluetooth). Технология стандартизирована, следовательно, проблемы несовместимости устройств от конкурирующих фирм быть не должно.

Bluetooth - это маленький чип, представляющий собой высокочастотный (2.4 - 2.48 ГГц) приёмопередатчик, работающий в диапазоне ISM (Industry, Science and Medicine; промышленный, научный и медицинский). Для использования этих частот не требуется лицензия (исключения рассмотрим ниже). Скорость передачи данных, предусматриваемая стандартом, составляет порядка 720 Кбит/с в асимметричном режиме и 420 Кбит/с в полнодуплексном режиме. Обеспечивается передача трех голосовых каналов, но не видеосигнала. Энергопотребление (мощность передатчика) не должно превышать 10 мВт. Изначально технология предполагала возможность связи на расстоянии не более 10 метров. Сегодня некоторые фирмы предлагают микросхемы Bluetooth, способные поддерживать связь на расстоянии до 100 метров. Как радиотехнология, Bluetooth способна "обходить" препятствия, поэтому соединяемые устройства могут находиться вне зоны прямой видимости. Соединение происходит автоматически, как только Bluetooth-устройства оказываются в пределах досягаемости, причем не только по принципу точка - точка (два устройства), но и по принципу точка - много точек (одно устройство работает с несколькими другими). Естественно, для реализации технологии Bluetooth на практике необходимо определенное программное обеспечение (ПО). Кстати, в новую версию операционной системы MS Windows Whistler встроена поддержка Bluetooth [17].

Передача данных Bluetooth

В стандарте Bluetooth предусмотрена дуплексная передача на основе разделения времени (Time Division Duplexing - TDD). Основное устройство передает пакеты в нечетные временные сегменты, а подчиненное устройство – в четные.

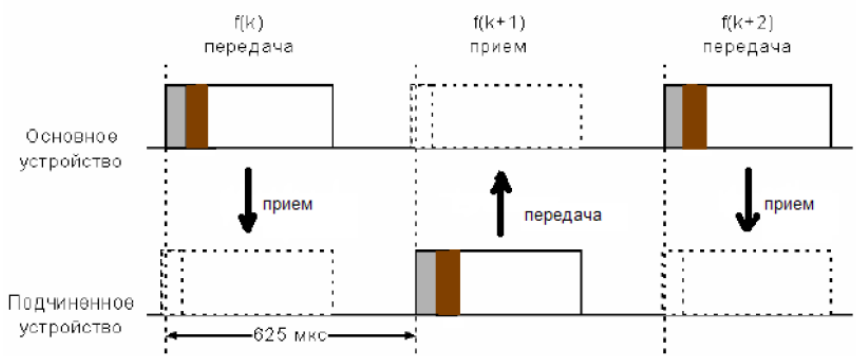


Рис. 7.87. Дуплексная передача с временным разделением

Пакеты в зависимости от длины могут занимать до пяти временных сегментов. При этом частота канала не меняется до окончания передачи пакета.

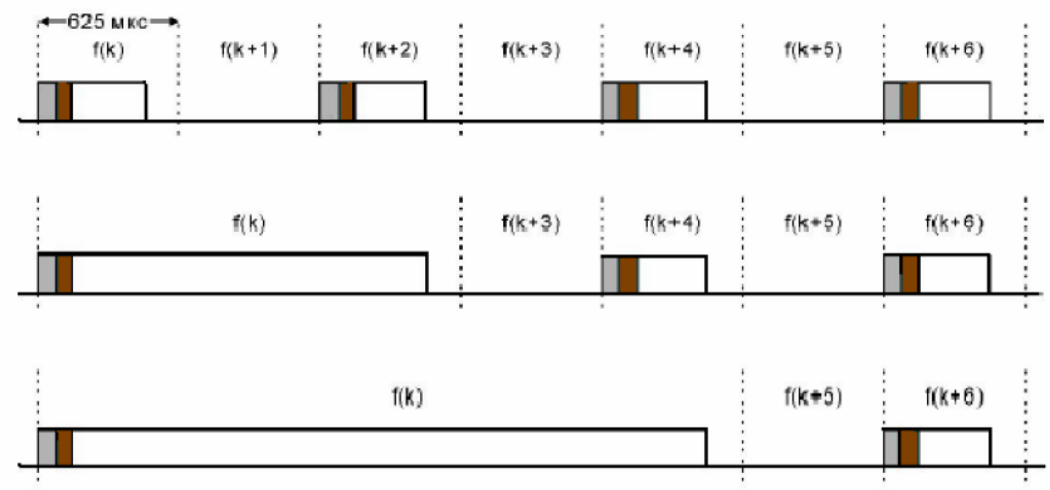


Рис. 7.88. Передача пакетов различной длины

Протокол Bluetooth может поддерживать асинхронный канал данных, до трех синхронных (с постоянной скоростью) голосовых каналов или канал с одновременной асинхронной передачей данных и синхронной передачей голоса. Скорость каждого голосового канала – 64 Кбит/с в каждом направлении, асинхронного в асимметричном режиме – до 723,2 Кбит/с в прямом и 57,6 кбит/с в обратном направлениях или до 433,9 Кбит/с в каждом направлении в симметричном режиме.

Структура пакета

Стандартный пакет Bluetooth содержит код доступа длиной 72 бита, 54-битный заголовок и информационное поле длиной не более 2745 бит. Однако пакеты могут быть различных типов. Так, пакет может состоять только из кода доступа (в этом случае его длина равна 68 битам) или кода доступа и заголовка.

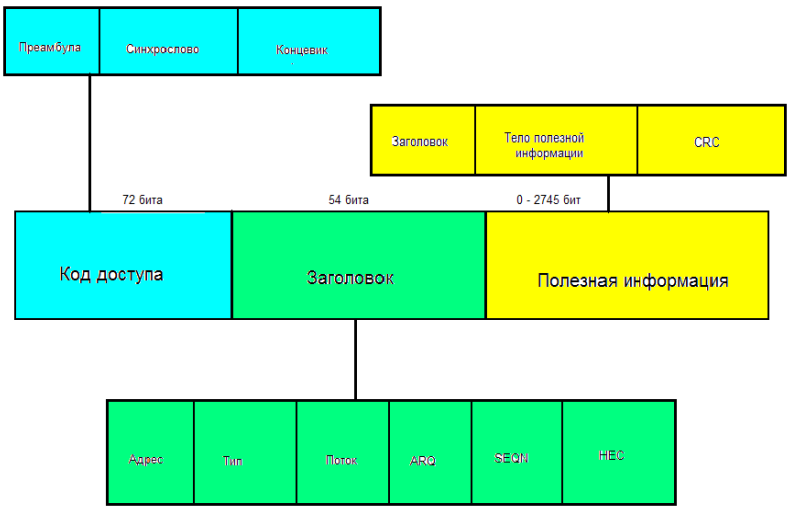


Рис. 7.89. Структура пакета

Код доступа идентифицирует пакеты, принадлежащие одной пикосети, а также используется для синхронизации и процедуры запросов. Он включает преамбулу (4 бита), синхрослово (64 бита) и концевик – 4 бита контрольной суммы.

Заголовок содержит информацию для управления связью и состоит из шести полей:

Адрес (3 бита) - адрес активного элемента;

Тип (4 бита) - код типа данных;

Поток (1 бит) - управление потоком данных, показывает готовность устройства к приему;

ARQ (1 бит) - подтверждение правильного приема;

SEQN (1 бит) - служит для определения последовательности пакетов;

HEC (8 бит) - контрольная сумма.

Заключительной частью общего формата пакета является полезная информация. В этой части есть два типа полей: поле голоса (синхронное) и поле данных (асинхронное). ACL пакеты имеют только поле данных, а SCO пакеты – только поле голоса. Исключением является пакет данных и голоса (Data Voice - DV), который имеет оба поля. Поле данных состоит из трех сегментов: заголовок полезной информации, тело полезной информации и возможно, CRC (Cyclic Redundancy Check) код.

Заголовок полезной информации (8 бит). Только поля данных имеют заголовокполезной информации. Он определяет логический канал, управление потоком в логических каналах, а также имеет указатель длины полезной информации.

Тело полезной информации (0-2721 бит). Тело полезной информации включает пользовательскую информацию. Длина этого сегмента указана в поле длины заголовка полезной информации.

CRC (16 бит). От передаваемой информации вычисляется 16-битный циклический избыточный код (CRC), после чего он прикрепляется к информации.

Существует 4 типа контрольных пакетов: NULL, POLL, FHS, ID. Они одинаковые как для ACL, так и для SCO.

ID-пакеты имеют длину 68 бит и применяются для пейджинга и запросов. Состоит из поля Код Доступа .

NULL-пакеты (126 бит) состоят только из полей Код Доступа и Заголовок, играя роль подтверждений установления соединения или получения данных

Тип POLL (126 бит) аналогичен предыдущему за исключением того, что POLL-пакеты обязывают получателя ответить.

Пакеты FHS (366 бит) содержат информацию об адресе, классе устройства и тактовой частоте его передатчика

Работа Bluetooth

Есть два основных состояния для устройств Bluetooth: Соединение (Connection) и Режим ожидания (Standby). Предусмотрено семь субсостояний, которые используются для

добавления клиента или подключения к пикосети: page, page scan, inquiry, inquiry scan, master response, slave response и inquiry response.

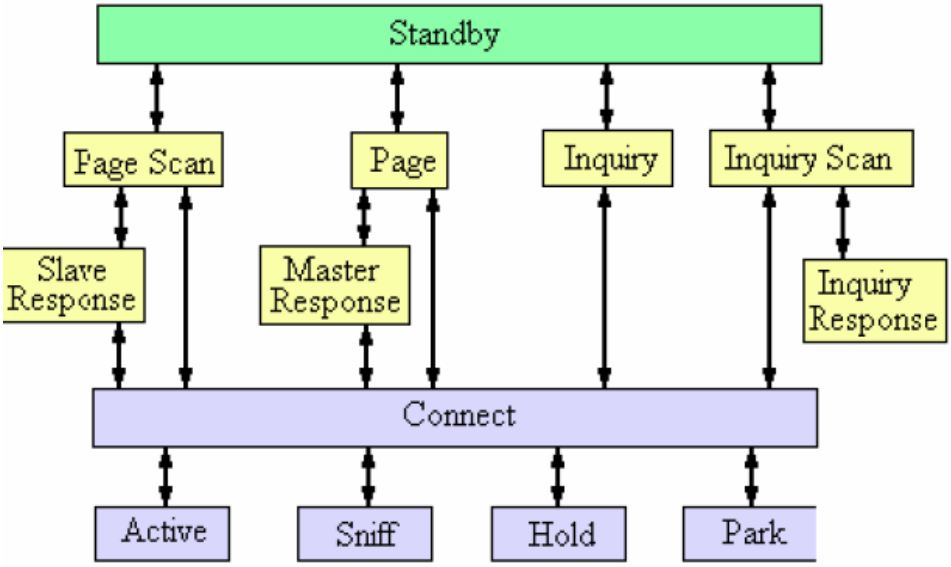


Рис. 7.60. Состояние соединений

Состояние Standby по умолчанию является режимом с пониженным энергопотреблением, работает только внутренний задающий генератор. В состоянии Соединения основной узел (master) и подчиненный (slave) могут обмениваться пакетами, используя код доступа к каналу.

Соединение между устройствами присходит так - если об удаленном устройстве ничего не известно, то используются процедуры inquiry и page. Если некоторая информация о устройстве все-таки есть, то достаточно процедуры page.

Этап 1

Процедура inquiry позволяет устройству определить, какие приборы доступны, выяснить адреса и осуществить синхронизацию.

1.1 Посылаются пакеты inquiry и получаются отклики.

1.2 Если адресат, получивший пакет inquiry, находится в состоянии inquiry scan , тогда он способен принимать такие пакеты

1.3 Получатель переходит в состояние inquiry response и посылает отправителю пакет-отклик.

После того как процедура inquiry завершена, соединение может быть установлено с помощью процедуры paging.

Этап 2

Процедура paging реализует соединение. Для осуществления этой процедуры необходим адрес. Устройство, выполняющее процедуру paging, атоматически становится хозяином этого соединения.

2.1 Посылается пакет paging

2.2 Адресат получет этот пакет (находится в состоянии page Scan)

2.3 Получатель посылает отправителю пакет-отклик (находится в состоянии Slave Response)

2.4 Инициатор посылает адресату пакет FHS (находится в состоянии Master Response).

2.5 Получатель посылает отправителю второй пакет-отклик (находится в состоянии Slave Response)

2.6 Получатель и отправитель устанавливают параметры канала заданные инициатором (находятся в состоянии Master Response & Slave Response)

После установления соединения основной узел (master) посылает пакет POLL, чтобы проверить, синхронизовал ли клиент свои часы и настроился ли на коммутацию частот. Клиент при этом может откликнуться любым пакетом. После успешного обнаружения устройств новое Bluetooth устройство получает набор адресов доступных Bluetooth устройств, после чего выясняет имена всех доступных Bluetooth устройств из списка. У каждого Bluetooth устройства есть свой глобально уникальный адрес, но на уровне пользователя обычно используется не этот адрес, а имя устройства, которое может быть любым, и ему не обязательно быть глобально уникальным. Имя Bluetooth устройства может быть длиной до 248 байт, и использовать кодовую страницу в соответствии с Unicode UTF-8 (при использовании UCS-2, имя может быть укорочено до 82 символов). Также у Bluetooth есть возможность автоматического подключения Bluetooth устройств к службам, предоставляемым другими Bluetooth устройствами. Поэтому, после того как имеется список имён и адресов, выполняется поиск доступных услуг, предоставляемых различными устройствами. Для поиска возможных услуг используется специальный протокол обнаружения услуг (Service Discovery Protocol - SDP).

Устройство Bluetooth при установлении соединения может работать в четырех режимах: Active (активный), Hold (удержание), Sniff (прослушивание) и Park (пассивный).

Таблица 7.12. Режимы работы Bluetooth

Название режима	Описание
Active	В активном режиме устройство Bluetooth участвует в работе канала. Основной узел (master) диспетчеризует обмены на основе запросов трафика, поступающих от участников. Кроме того, этот режим предусматривает регулярные обмены с целью синхронизации клиентов. Активные клиенты прослушивают домены master-to-slave пакетов. Если к активному клиенту нет обращений, он может пребывать в пассивном состоянии (sleep) до

	очередной передачи со стороны главного узла
Sniff	Устройства синхронизованные в рамках пикосети могут перейти в режим экономного расходования энергии, когда их активность понижается. В режиме SNIFF, подчиненное устройство прослушивает пикосеть с пониженной частотой. Этот режим имеет наивысшую скважность рабочего цикла (наименьшая экономия энергии) из 3 экономичных режимов (sniff, hold и park)
Hold	Устройства синхронизованные в рамках пикосети могут перейти в режим экономного расходования энергии, когда их активность понижается. Основной узел пикосети может перевести клиента в режим HOLD, когда работает только внутренний таймер. Подчиненное устройство может запросить перевода в режим HOLD. Передача данных возобновляется мгновенно, когда устройство выходит из режима HOLD. Клиент имеет промежуточную скважность (промежуточный уровень экономии энергии) из указанных 3 режимов (sniff, hold и park)
Park	В режиме PARK, устройство еще синхронизовано в рамках пикосети, но не принимает участия в обменах. Пассивные устройства отказываются от своих MAC-адресов, прослушивают трафик главного модуля с целью ресинхронизации и отслеживают широковещательные сообщения. Данный режим имеет минимально возможную скважность (максимальная экономия энергии) из указанных 3 режимов (sniff, hold и park). Устройства, находящиеся в режиме park, должны посылать пакеты широковещательно, так как лишены собственного активного адреса.

"Частотный конфликт"

Тот факт, что частотный диапазон 2.4 ГГц свободен от лицензирования, вносит определенные сложности в использование Bluetooth-устройств. В этом диапазоне работают также различные медицинские приборы, бытовая техника, беспроводные телефоны, беспроводные локальные сети стандарта IEEE. Вполне логично предположить, что они могут "конфликтовать" друг с другом. Во избежание интерференции с другими беспроводными устройствами Bluetooth работает по принципу скачкообразной перестройки частоты (1600

скачков в секунду). Переход с одной частоты на другую происходит по псевдослучайному алгоритму. Это позволяет "освободить" нужные другим устройствам частоты[3].

Моделирование Bluetooth

Модель состоит из трех основных блоков:

Передатчик;

Канал;

Приемник.

Канал имеет три режима работы:

Нет канала;

AWGN канал;

Также имеется генератор сигнала стандарта 802.11, который как раз может конфликтовать с сигналами Bluetooth, для чего и применяется скачкообразная перестройка частоты.

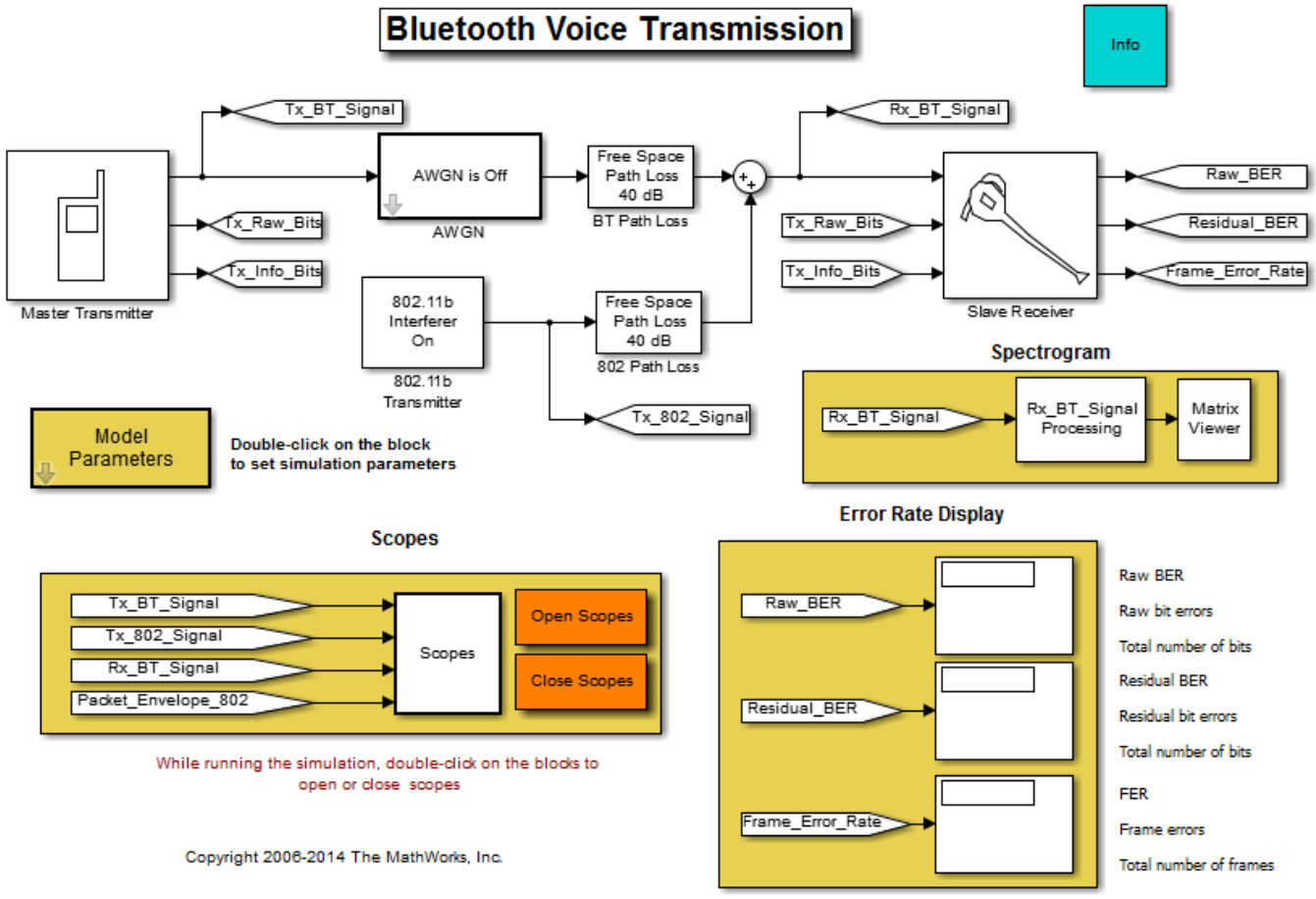


Рис. 7.61. Модель Bluetooth в MATLAB R2015b

Результаты моделирования.

В результате моделирования данной схемы система строит три графика: спектр сигнала, временную форму сигнала и зависимость изменения рабочей частоты во времени(скачкообразная перестройка). На графике ниже представлен спектр Bluetooth сигнала в один из моментов времени. Одним из минусов метода перестройки частоты в

системе Bluetooth являются задержки, которые хорошо видны на данной диаграмме при моделировании, также о них будет сказано ниже.

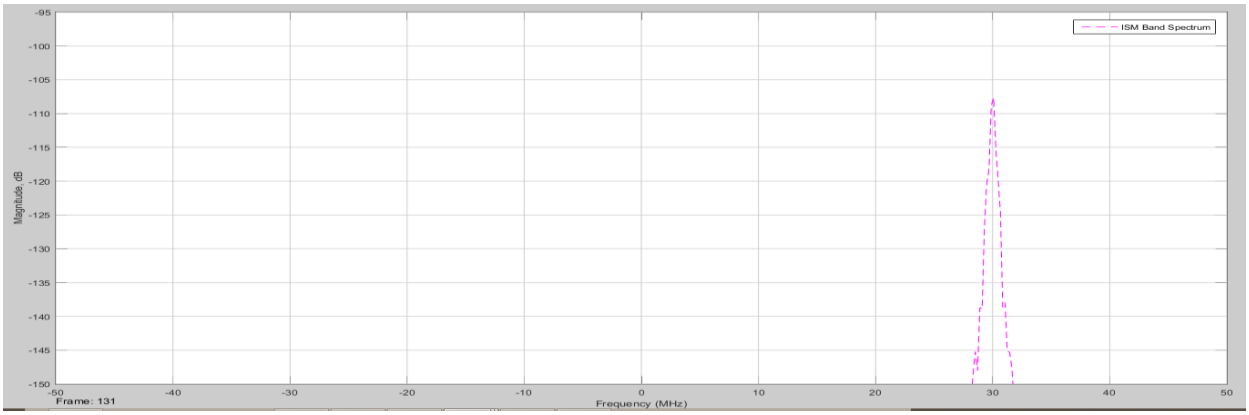


Рис. 7.61. Спектр Bluetooth без мешающего сигнала 802.11

Временная форма сигнала представляет просто набор битов, как и во многих современных системах связи. О значениях каждого бита(структуре кадра) была сказано ранее.

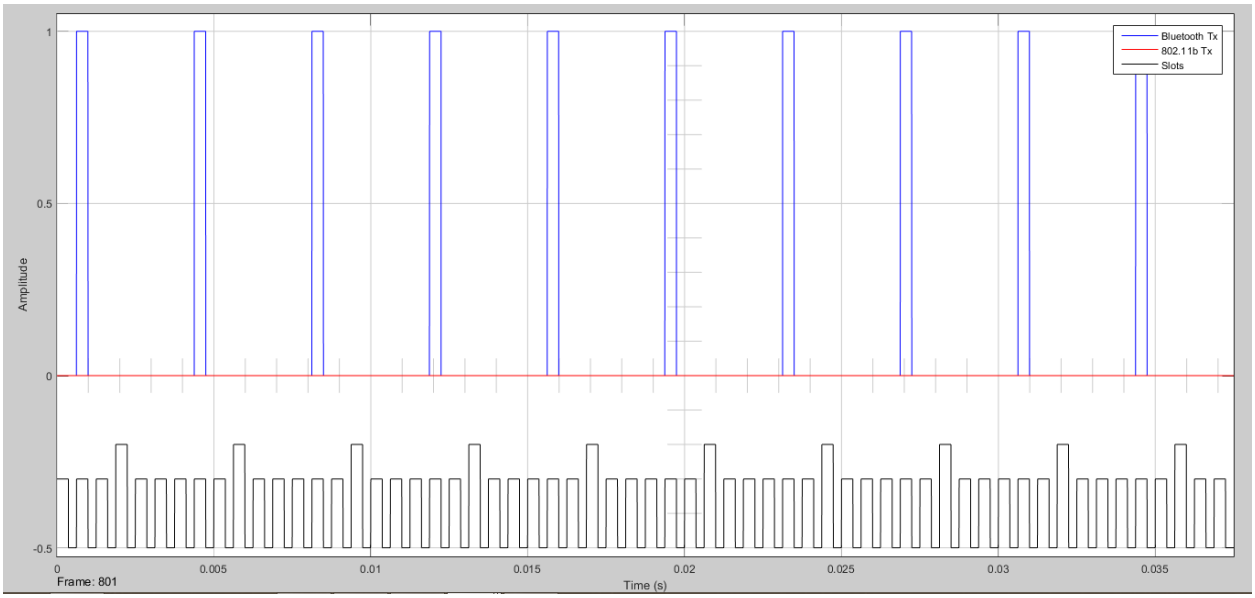


Рис. 7.62. Временная диаграмма Bluetooth без мешающего сигнала 802.11

На рисунке 7.63 хорошо видно изменение частоты от времени. На рисунке на оси абсцисс представлена частота, а на оси ординат время. Видно, что по оси времени перестройка с одной частоты на другую занимает определенное время, что относят к недостаткам системы Bluetooth.

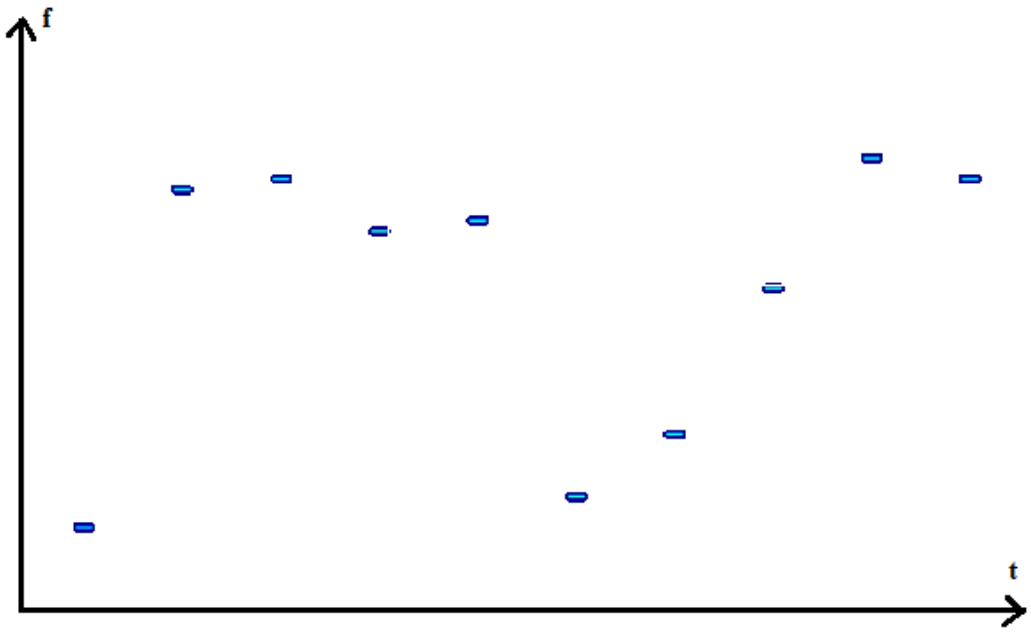


Рис. 7.63. Пример скачков частоты Bluetooth во времени без мешающего сигнала 802.11(WiFi)

На рисунке 7.64 представлен спектр вместе с мешающим сигналам. Здесь прекрасно видно, почему для построения системы Bluetooth был выбран алгоритм FHSS, который позволяет ему работать в одном диапазоне частот со стандартом 802.11 не мешая друг другу.

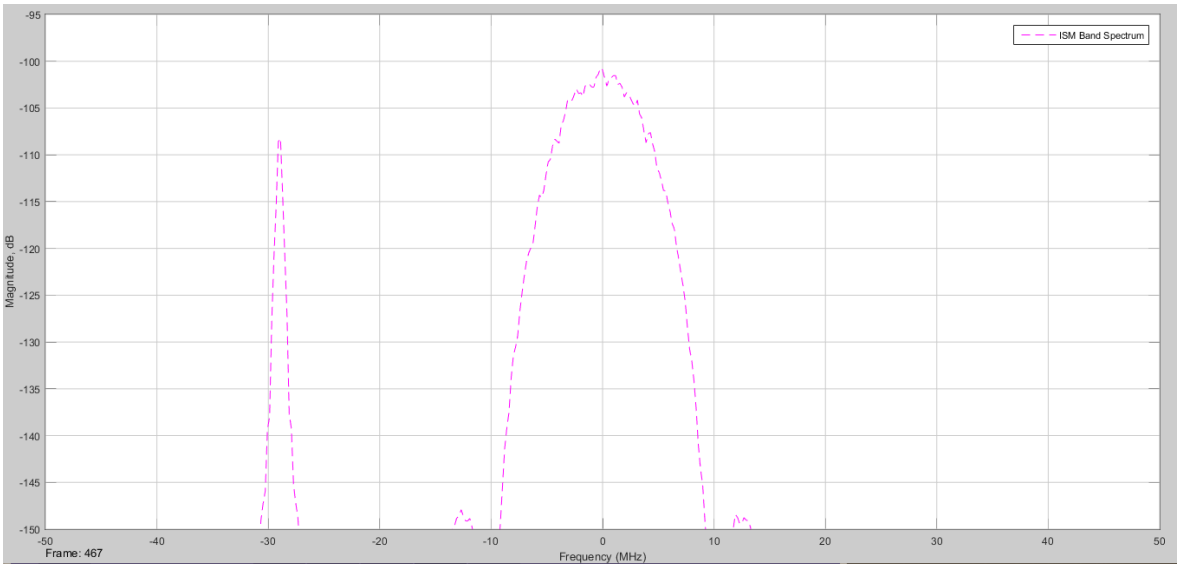


Рис. 7.64. Спектр Bluetooth с мешающим сигналом 802.11

Благодаря тому, что спектры сигналов разнесены в частотной области перекрытие их во временной, не играет большой роли, т.к. сигналы можно без проблем разделить.

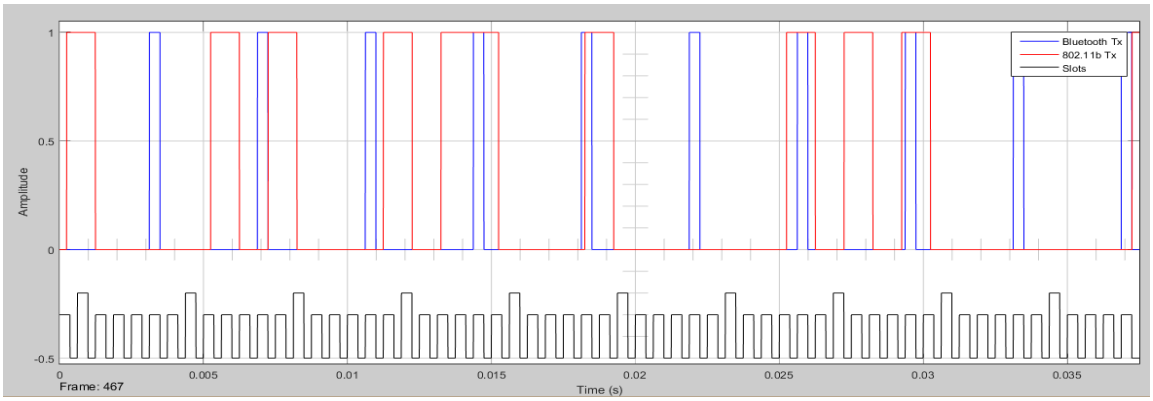


Рис. 7.65. Временная диаграмма Bluetooth с мешающим сигналом 802.11

Из рисунка ниже прекрасно видно, что во время работы устройства стандарта 802.11 рабочая частота системы Bluetooth находится достаточно далеко по спектру, а в некоторые моменты занимает свободный диапазон стандарта 802.11

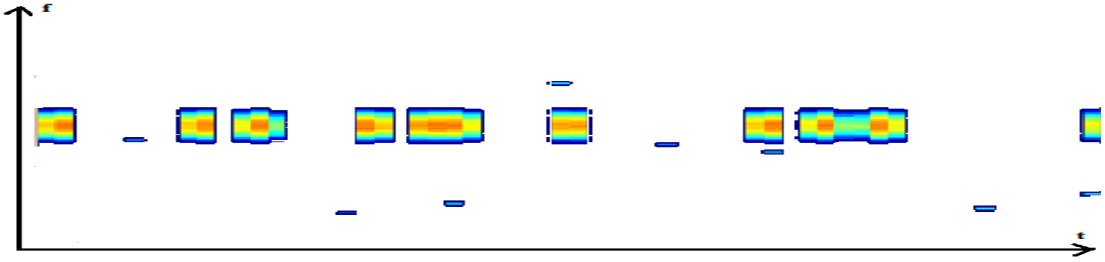


Рис. 7.66. Пример скачков частоты Bluetooth во времени с мешающим сигналом 802.11

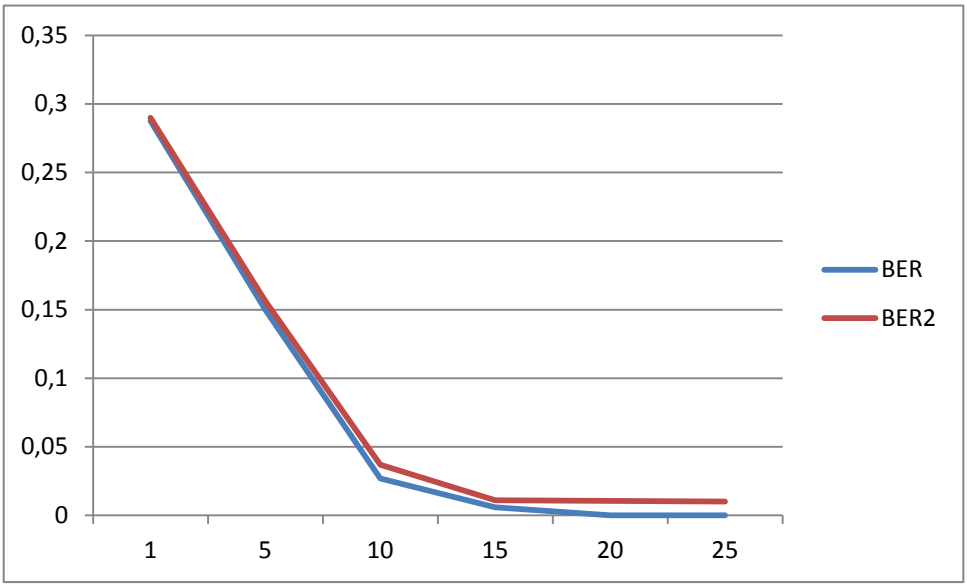


Рис. 7.67. Зависимость BER от SNR. Красным цветом (верхняя кривая) выделен график при включенном мешающем сигнале 802.11

Благодаря алгоритму FHSS система не сильно подвержена влиянию других стандартов передачи данных, работающих в том же диапазоне частот.

В разделе покана технология передачи данных 802.15.1 Bluetooth, а также использована модель передачи звука по такой системе в системе Simulink.

С помощью модели были построены временная диаграмма сигнала, спектр и FHSS спектр сигнала BLUETOTH при воздействии мешающего сигнала и без него. Также была построена зависимость BER от SNR.

На основе графиков зависимости BER от SNR (рисунок 5.67) видно,что мешающий сигнал 802.11 оказывает незначительное влияние на передачу данных. На рисунке 5.66 видно, что во время передачи сигнала 802.11, сигнал Bluetooth совершает скачок на другую частоту, что также хорошо видно на рисунке 7.64.

7.6. Имитационное моделирование системы мобильной связи стандарта IEEE 802.16 (WiMAX)

Существующие системы проводной цифровой связи уже не могут в полной мере удовлетворять растущим потребностям высокоскоростного широкополосного доступа. Важнейшими их недостатками являются длительные сроки прокладки, сложности расширения, высокие затраты, проблема "последней мили". Основной и является так называемая проблема "последней мили". Высокоскоростные цифровые соединительные линии DSL (Digital Subscriber Line) не снимают этой проблемы.

Технология WiMAX позволяет разрешить эту проблему в кратчайшие сроки, так как не требует прокладки соединительных линий к зданиям. Значительно проще развернуть по городу сеть базовых станций (наподобие сети станций сотовой связи). Каждая базовая станция в типовом варианте покрывает зону радиусом 6—8 км (возможны зоны радиусом до 30—50 км). В этой зоне каждая базовая станция (BS) по схеме "точка-многоточка" способна передавать/принимать сигналы от сотен зданий, внутри которых находится телекоммуникационное оборудование пользователей.

Под аббревиатурой WiMAX (Worldwide Interoperability for Microwave Access) понимается технология операторского класса с высоким качеством сервиса, которая основана на семействе стандартов IEEE 802.16, разработанных международным институтом инженеров по электротехнике и электронике (IEEE). Обеспечивает мультисервисность, гибкое распределение частот, задание приоритетов различным видам трафика, возможность обеспечения разного уровня качества (QoS), поддержка интерфейсов IP. Эта технология позволяет параллельно передавать голос, мультимедийную информацию и цифровые данные по одному каналу связи. Важным преимуществом является возможность быстро наращивать емкость и расширять территорию связи.

Технология WiMAX представляет прекрасную возможность обеспечивать беспроводной доступ всем пользователям цифрового оборудования, включая оборудование

беспроводных локальных сетей, технологии Wi-Fi, к глобальным сетям, являясь связующим звеном между локальными сетями и глобальными сетями.

При переходе к созданию систем широкополосного радиодоступа с интеграцией услуг стало понятно, что основополагающие принципы, заложенные в беспроводные системы на предыдущих этапах, нуждаются в существенной корректировке. На сигнальном уровне первостепенное значение приобрело оптимальное использование спектрального ресурса радиоканала при любых соотношениях “скорость - помехоустойчивость”. На уровне протоколов стало необходимым обеспечивать заданный уровень качества обслуживания каждому абоненту сети.

Основным преимуществом сетей WiMAX по сравнению с другими технологиями, призванными решать аналогичные задачи, является относительно быстрое развертывание систем на достаточно больших территориях без проведения работ по прокладке кабеля и предоставление конечным пользователям каналов связи в единицы Мбит/с, что особенно актуально для мест с неразвитой сетевой инфраструктурой. Основным конкурентом сетей WiMAX являются системы связи четвертого поколения LTE E UTRA.

На сегодняшний день беспроводные сети городского масштаба представлены следующими стандартами:

- IEEE 802.16e-2005, 2009 (WiMAX);
- ETSI HiperMAN;
- IEEE 802.20 (WBWA).

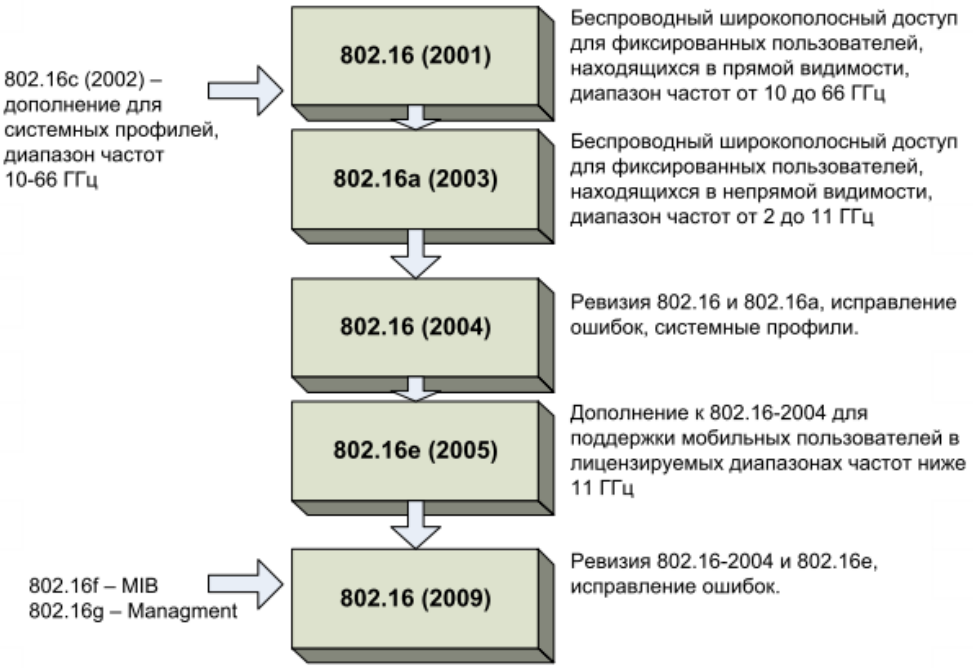


Рисунок 7.68 – Эволюция стандартов IEEE 802.16

Таблица 7.13 – Краткие характеристики стандартов, входящих в семейство IEEE 802.16

Название стандарта	**IEEE 802.16**	**IEEE 802.16a**	**IEEE 802.16e**
Частотный диапазон	10-66 ГГц	2-11 ГГц	2-6 ГГц
Скорость передачи информации	32-135 Мбит/с	до 75 Мбит/с	до 15 Мбит/с
Модуляция	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM
Ширина полосы частот	20, 25 и 28 МГц	Регулируемая 1,5 – 20 МГц	Регулируемая 1,5 – 20 МГц
Радиус действия	2-5 км	7-10 км, макс. радиус 50 км	2-5 км
Условия работы	Прямая видимость	Работа на отраженных лучах	Работа на отраженных лучах

Для обеспечения работоспособности систем в диапазоне 10-66 ГГц, вследствие относительно малой длины волны, требуется наличие прямой видимости между передатчиком и приемником. В таких условиях при анализе канала связи многолучевостью среды можно пренебречь. Данные передаются на одной несущей. Ширина полосы частот одного канала составляет 20, 25 или 28 МГц, что позволяет достигать скорости передачи данных до 135 Мбит/с.

В диапазоне частот 2-11 ГГц за счет увеличения длины волны возможен сценарий взаимодействия передатчика и приемника в условиях отсутствия прямой видимости. При этом необходимо применять более сложные (по сравнению с системами, функционирующими в диапазоне частот 10-66 ГГц) методы регулировки мощности, различные способы борьбы с межсимвольной интерференцией. Для передачи данных используется одна или множество несущих (сигналы с OFDM).

Необходимо различать стандарты связи серии IEEE 802.16 и форум WiMAX. Стандарты серии IEEE 802.16 — это множество стандартов, определяющих беспроводные сети городского масштаба (WMAN — Wireless Metropolitan Area Network), разработаны для обеспечения беспроводным широкополосным доступом стационарных и мобильных пользователей. Форум WiMAX является некоммерческой организацией для продвижения и сертификации устройств беспроводного широкополосного доступа, основанных на согласованном стандарте IEEE 802.16/ETSI HiperMAN. Сотрудничает с поставщиками услуг,

производителями оборудования, производителями тестового оборудования, сертификационными лабораториями и поставщиками программно-аппаратных ресурсов для обеспечения соответствия ожиданиям заказчика и государственным стандартам.

Стандарты серии IEEE 802.16 определяет радиоинтерфейс для систем широкополосного беспроводного доступа (уровни MAC и PHY, рисунок 2.3) с фиксированными и мобильными абонентами в диапазоне частот 1-66 ГГц, рассчитанных на внедрение в городских распределенных беспроводных сетях операторского класса. Сети, построенные на основе этих стандартов, займут промежуточной положение между локальными сетями (IEEE 802.11x) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE 802.20. Указанные стандарты совместно со стандартом IEEE 802.15 (PAN — Personal Area Network) и IEEE 802.17 (мосты уровня MAC) образуют иерархию стандартов беспроводной связи.

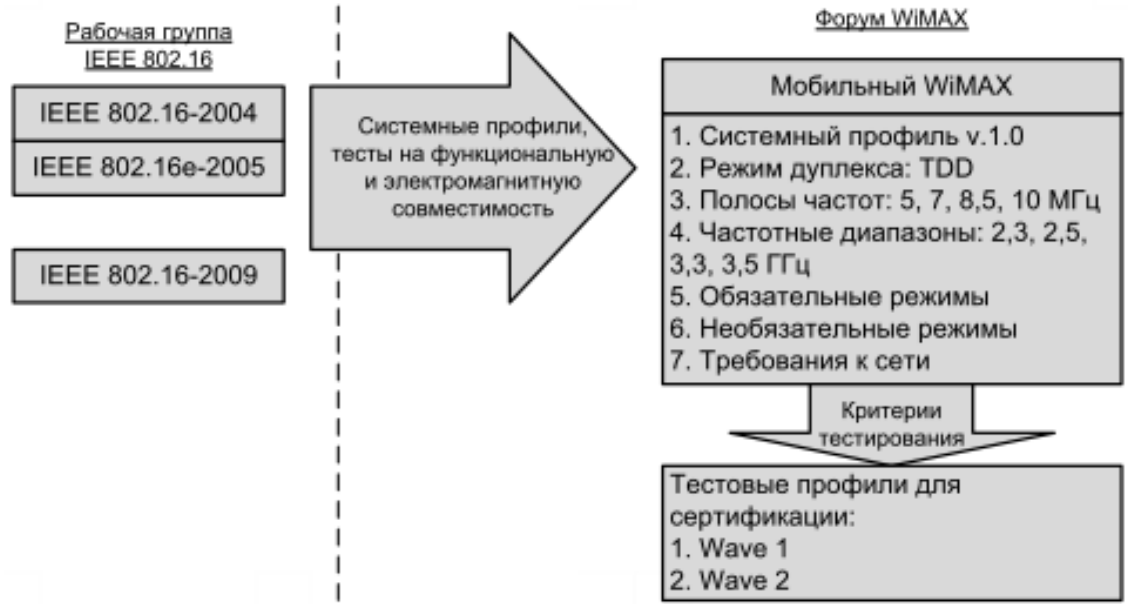


Рисунок 7.67 – Стандарты серии IEEE 802.16 и форум WiMAX

Структура стандартов IEEE 802.16 представлена на рисунке 2.3. Стандарты описывают MAC- и PHY- уровни семиуровневой эталонной модели взаимодействия открытых систем (ЭМВОС). При этом уровень MAC делится на подуровни конвергенции, общей части и безопасности.

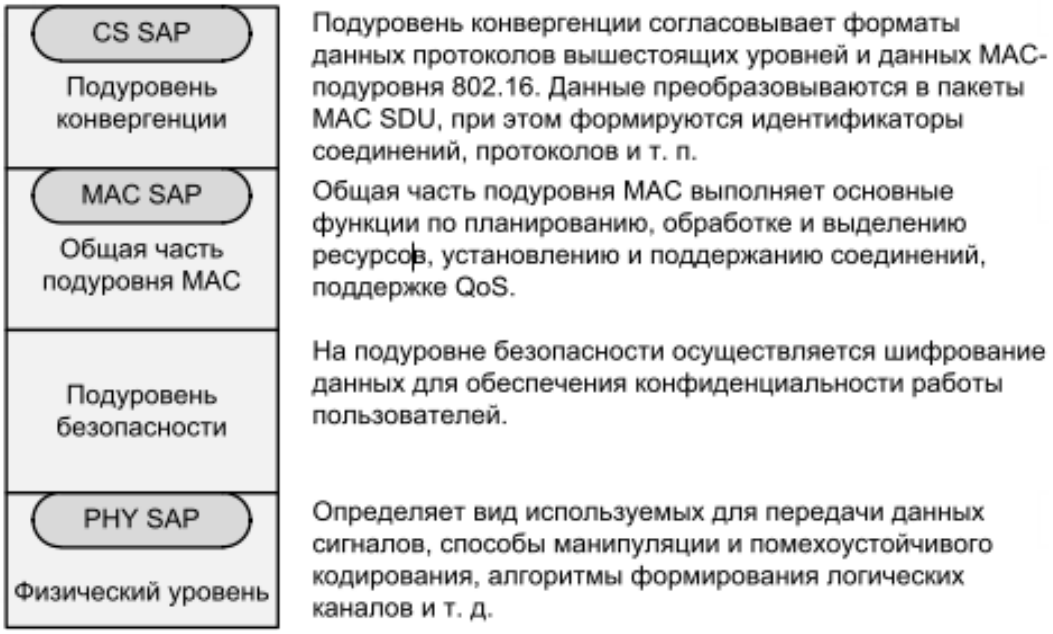


Рисунок 7.68 – Структура стандартов IEEE 802.16

Архитектура сетей WiMAX IEEE 802.16. Сетевой уровень

Базовая станция (БС, BS — Base Station) размещается в здании или на вышке и осуществляет связь с абонентскими станциями (АС, SS —Subscriber Station) по схеме — «точка – мультиточка» (Point to Multipoint —PMP). Возможен сеточный режим связи (Mesh — сетка связей — «точка – точка» — PTP), когда любые клиенты (АС) могут осуществлять связь между собой непосредственно, а антенные системы, как правило, являются ненаправленными. БС предоставляет соединение с основной сетью и радиоканалы к другим станциям. Радиус действия БС может достигать 30 км (в случае прямой видимости) при типовом радиусе сети 6–8 км. АС может быть радиотерминалом или повторителем, который используется для организации локального трафика. Трафик может проходить через несколько повторителей, прежде чем достигнет клиента. Антенны в этом случае являются направленными.

Канал связи предполагает наличие двух направлений передачи: восходящий канал (АС – БС, uplink) и нисходящий (БС – АС, downlink). Эти два канала используют разные неперекрывающиеся частотные диапазоны при частотном дуплексе и различные интервалы времени при временном дуплексе.

Простейший способ представления архитектуры сетей WiMAX заключается в их описании как совокупности БС, которые располагаются на крышах высотных зданий или вышках, и клиентских приемо-передатчиков (рисунок 2.4).

Рисунок 7.69 – Схематичное изображение сети WiMAX

Радиосеть обмена данными между БС и АС работает в СВЧ-диапазоне от 2 до 11 ГГц. Такая сеть в идеальных условиях может обеспечить техническую скорость передачи информации до 75 Мбит/с и не требует того, чтобы БС находилась на расстоянии прямой видимости от пользователя.

Диапазон частот от 10 до 66 ГГц используется для установления соединения между соседними базовыми станциями при условии, что они располагаются в зоне прямой видимости друг от друга. Так как в городской среде это условие может оказаться невыполнимым, связь между базовыми станциями иногда организуют посредством прокладки кабелей.

При более детальном рассмотрении сеть WiMAX можно описать как совокупность беспроводного и базового (опорного) сегментов. Первый описывается в стандарте IEEE 802.16, второй определяется спецификациями WiMAX Forum. Базовый сегмент объединяет все аспекты, не относящиеся к абонентской радиосети, то есть связь базовых станций друг с другом, связь с локальными сетями. Базовый сегмент основывается на IP-протоколе и стандарте IEEE 802.3-2005 (Ethernet). Однако само описание архитектуры в части, не относящейся к беспроводной клиентской сети, содержится в документах WiMAX Forum, объединенных под общим названием – "Network Architecture".

Таблица 7.14 – Основные режимы для стандарта IEEE 802.16 в РФ

Диапазон частот, ГГц	Разрешенные полосы частот, МГц	Общая ширина выделенных полос,	Тип беспроводного доступа

		МГц	
2,5	2500 – 2530 2560 – 2570 2620 – 2630 2660 – 2670 2680 – 2690	70	мобильный
3,5	3400 – 3450 3500 – 3550	100	фиксированный
5	5150 – 5350 5650 – 5725 5725 – 6425	975	фиксированный

В этих спецификациях к сетям WiMAX предъявляются такие требования, как независимость архитектуры от функций и структуры транспортной IP-сети. В то же время, должны обеспечиваться услуги, основанные на применении IP-протокола, а также мобильная телефония на основе VoIP и мультимедийные услуги. Обязательным является условие поддержки архитектурой протоколов IPv4 и IPv6. Сети WiMAX должны быть легко масштабируемыми и гибко изменяемыми и основываться на принципе декомпозиции (строиться на основе стандартных логических модулей, объединяемых через стандартные интерфейсы). Свойства масштабируемости и гибкости необходимо обеспечивать по таким эксплуатационным характеристикам, как плотность абонентов, географическая протяженность зоны покрытия, частотные диапазоны, топология сети, мобильность абонентов. Сети WiMAX должны поддерживать взаимодействие с другими беспроводными или проводными сетями. Большое значение имеет способность обеспечивать различные уровни качества обслуживания QoS.

Физический уровень WiMAX

На физическом уровне систем WiMAX над передаваемыми битами осуществляются следующие канальные процедуры (рисунок 2.5): скремблирование (рандомизация), помехоустойчивое кодирование, перемежение, кодирование повторением и модуляция.

Полученные модуляционные символы делятся на логические подканалы, и с использованием ОБПФ формируется отсчет передаваемого OFDMA-символа.

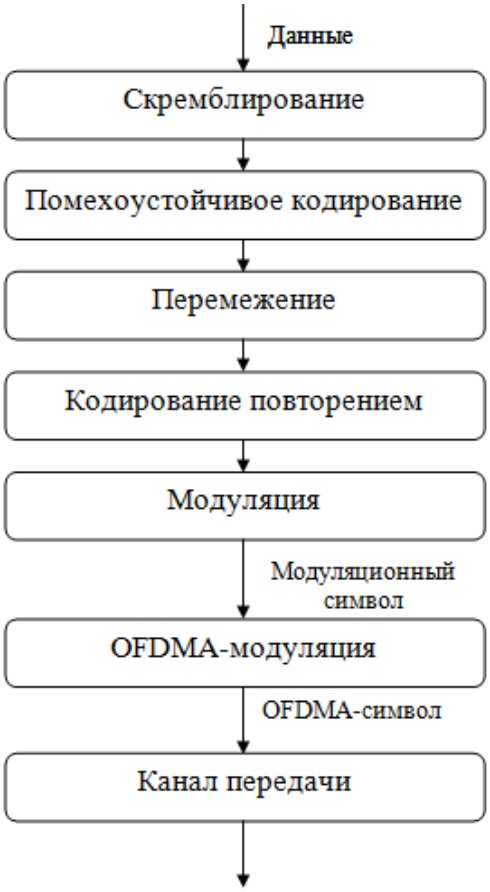


Рисунок 7.70 – Преобразования данных на физическом уровне WiMAX

На физическом уровне в стандарте IEEE 802.16-2004 определены три метода передачи данных: метод модуляции одной несущей (SC), метод ортогонального частотного мультиплексирования (OFDM) и метод множественного доступа на основе такого мультиплексирования (OFDMA) [2].

Спецификация физического уровня WirelessMAN-OFDM является наиболее интересной с точки зрения практической реализации. Она базируется на технологии OFDM, что значительно расширяет возможности оборудования, в частности, позволяет работать на относительно высоких частотах в условиях отсутствия прямой видимости. Кроме того, в нее включена поддержка топологии «каждый с каждым» (mesh) [3], при которой абонентские устройства могут одновременно функционировать и как базовые станции, что сильно упрощает развертывание сети и помогает преодолеть проблемы прямой видимости.

Скремблирование

Скремблирование — это сложение по модулю два передаваемых битов с элементами ПСП, которую формирует генератор ПСП с задающим полиномом вида $x^{15} + x^{14} + 1$. Генератор ПСП инициализируется вектором 011011100010101.

Скремблирование осуществляется только над информационными битами Причем при скремблировании каждого блока данных, подлежащих помехоустойчивому кодированию,

сдвигающий регистр скремблера инициализируется заново. Байты данных поступают на вход скремблера начиная со старшего значащего разряда.

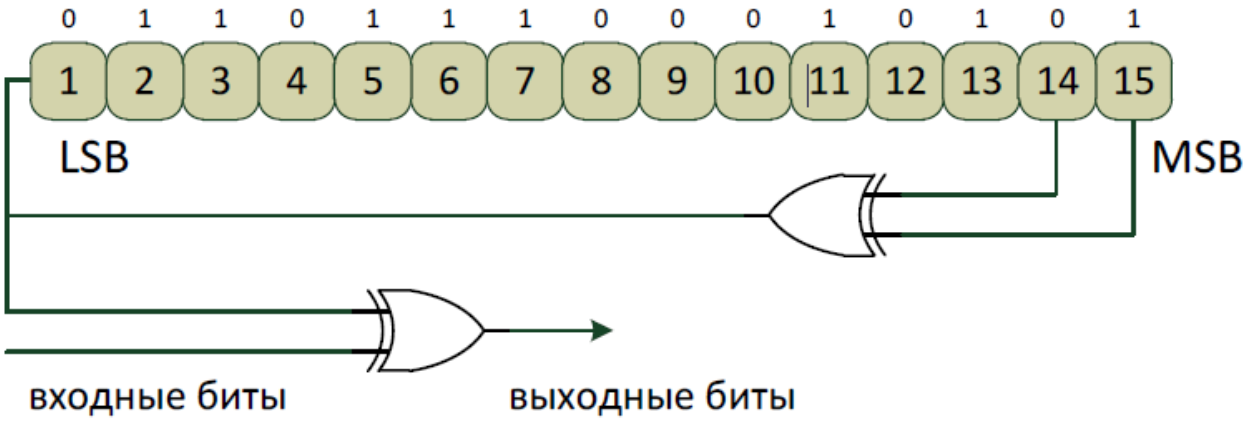


Рисунок 7.71 – Схема скремблера

Помехоустойчивое кодирование

Многолучевое распространение радиосигнала может приводить к ослаблению и даже полному подавлению некоторых поднесущих вследствие интерференции прямого и задержанного сигналов. Для решения этой проблемы используется помехоустойчивое кодирование. В стандарте IEEE 802.16-2004 предусмотрены как традиционные технологии помехоустойчивого кодирования, так и относительно новые методы. К традиционным относится сверточное кодирование с декодированием по алгоритму Витерби и коды Рида-Соломона. К относительно новым — блочные и сверточные турбокоды.

Перемежение

После осуществления скремблирования и помехоустойчивого кодиро-вания, над битами каждого блока должно быть выполнено двухэтапное пе-ремежение. Первый этап гарантирует, что соседние в исходной последова-тельности биты будут распределены не в соседние поднесущие. Второй этап обеспечивает распределение соседних битов или в наиболее, или в наименее значимые биты сигнального созвездия, что предотвратит дли-тельные последовательности наименее надежных битов.

Модуляция

В системах беспроводного широкополосного доступа используют сигналы как двоичной (ФМ-2), так и многопозиционной (ФМ-4, КАМ-16, КАМ-64 и т. п.) модуляции. Сигналы многопозиционной фазовой модуляции (МФМ) характеризуются высокой частотной эффективностью, однако при этом вследствие уменьшения евклидовых расстояний между сигнальными точками существенно снижается помехоустойчивость приема, что при фиксированной вероятности ошибки эквивалентно ухудшению энергетической эффективности. Сигналы КАМ являются некоторым компромиссом,

выигрывая у МФМ по энергетической эффективности, но уступая по спектральной, что может компенсироваться применением помехоустойчивого кода. По этой причине в сетях WiMAX IEEE 802.16e-2005, 2009 применяются методы модуляции ФМ-2, ФМ-4, КАМ-16 и КАМ-64.

При отображении бит на сигнальную плоскость применяется манипуляционный код Грея. Соответствующие сигнальные созвездия представлены на рисунке 7.72.

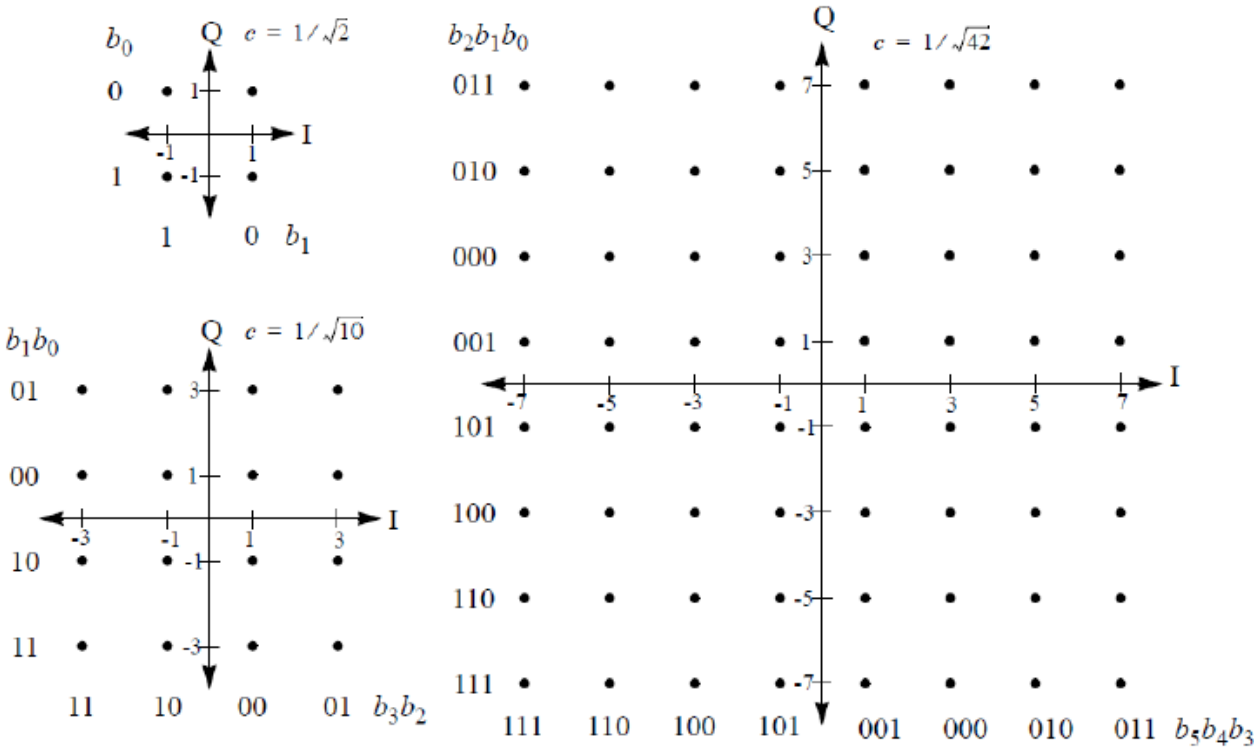


Рисунок 7.72 – Сигнальные созвездия, соответствующие методам модуляции ФМ-4, КАМ-16 и КАМ-64, IEEE 802.16e-2005

Модуляция OFDM

При формировании OFDM-сигнала цифровой поток данных делится на несколько подпотоков, и каждая поднесущая связывается со своим подпотоком данных. Амплитуда и фаза поднесущей вычисляются на основе выбранной схемы модуляции. Согласно стандарту, отдельные поднесущие могут модулироваться с использованием бинарной фазовой манипуляции (BPSK), квадратурной фазовой манипуляции (QPSK) или квадратурной амплитудной манипуляции (QAM) порядка 16 или 64. В передатчике амплитуда как функция фазы преобразуется в функцию от времени с помощью обратного быстрого преобразования Фурье (ОБПФ). В приемнике с помощью быстрого преобразования Фурье (БПФ) осуществляется преобразование амплитуды сигналов как функции от времени в функцию от частоты.

Применение преобразования Фурье позволяет разделить частотный диапазон на поднесущие, спектры которых перекрываются, но остаются ортогональными. Ортогональность поднесущих означает, что каждая из них содержит целое число колебаний на период передачи символа. Как видно на рисунке 7.73, спектральная кривая любой из поднесущих имеет нулевое значение для «центральной» частоты смежной кривой. Именно эта особенность спектра поднесущих и обеспечивает отсутствие между ними интерференции.

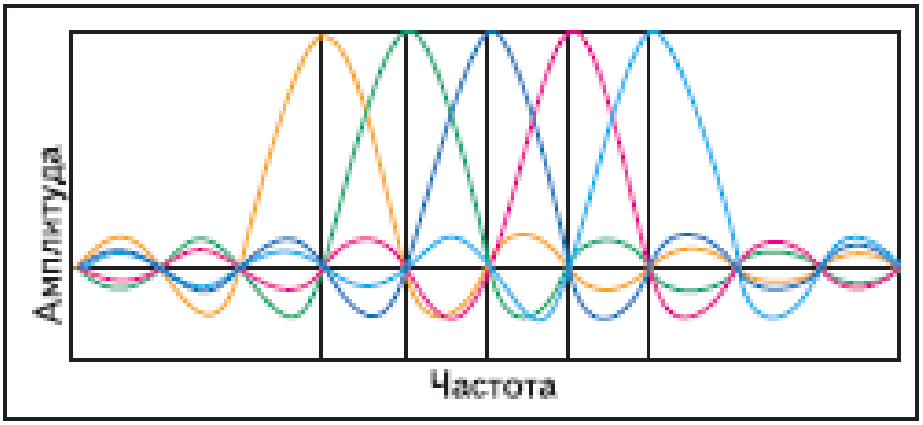


Рисунок 7.73 – Ортогональные поднесущие

Одним из главных преимуществ метода OFDM является его устойчивость к эффекту многолучевого распространения. Эффект вызывается тем, что излученный сигнал, отражаясь от препятствий, приходит к приемной антенне разными путями, вызывая межсимвольные искажения. Этот вид помех характерен для городов с разноэтажной застройкой из-за многократных отражений радиосигнала от зданий и других сооружений. Для того чтобы избежать межсимвольных искажений, перед каждым OFDM-символом вводится защитный интервал, называемый циклическим префиксом. Циклический префикс представляет собой фрагмент полезного сигнала, что гарантирует сохранение ортогональности поднесущих (но только в том случае, если отраженный сигнал при многолучевом распространении задержан не больше, чем на длительность циклического префикса). Кроме того, циклический префикс позволяет выбрать окно для преобразования Фурье в любом месте временного интервала символа (рисунок 7.74).

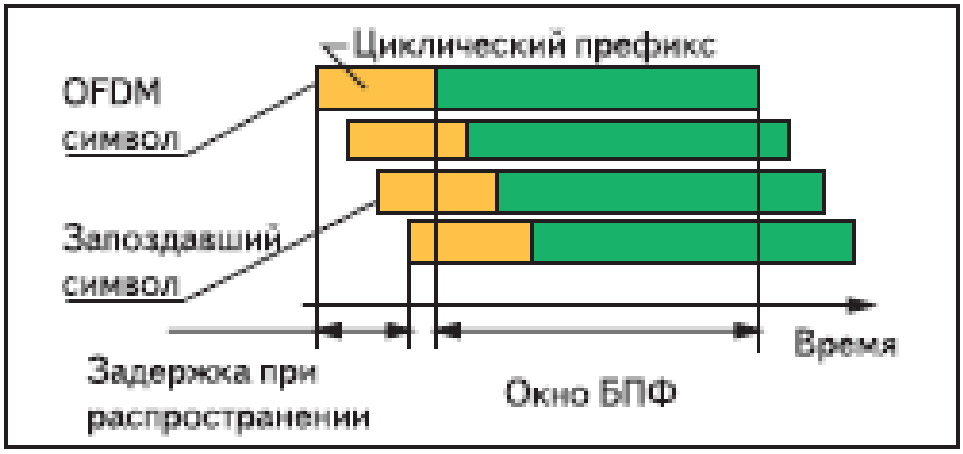


Рисунок 7.74– Обработка OFDM-символа при многолучевом распространении

Защита информации

В соответствии со стандартом, для предотвращения несанкционированного доступа и защиты пользовательских данных осуществляется шифрование всего передаваемого по сети трафика. Базовая станция (БС) WiMAX представляет собой модульный конструктив, в который при необходимости можно установить несколько модулей со своими типами интерфейсов, но при этом должно поддерживаться административное программное обеспечение для управления сетью. Данное программное обеспечение обеспечивает централизованное управление всей сетью. Логическое добавление в существующую сеть абонентских комплектов осуществляется также через эту административную функцию.

Абонентская станция (АС) представляет собой устройство, имеющее уникальный серийный номер, MAC-адрес, а также цифровую подпись X.509, на основании которой происходит аутентификация АС на БС. При этом, согласно стандарту, срок действительности цифровой подписи АС составляет 10 лет. После установки АС у клиента и подачи питания АС авторизуется на базовой станции, используя определенную частоту радиосигнала, после чего базовая станция, основываясь на перечисленных выше идентификационных данных, передает абоненту конфигурационный файл по TFTP-протоколу. В этом конфигурационном файле находится информация о поддиапазоне передачи (приема) данных, типе трафика и доступной полосе, расписание рассылки ключей для шифрования трафика и прочая необходимая для работы АС информация. Необходимый файл с конфигурационными данными создается автоматически, после занесения администратором системы АС в базу абонентов, с назначением последнему определенных параметров доступа.

После процедуры конфигурирования аутентификация АС на базовой станции происходит следующим образом:

1. Абонентская станция посылает запрос на авторизацию, в котором содержится сертификат X.509, описание поддерживаемых методов шифрования и дополнительная информация.

2. Базовая станция в ответ на запрос на авторизацию (в случае достоверности запроса) присылает ответ, в котором содержится ключ на аутентификацию, зашифрованный открытым ключом абонента, 4-битный ключ для определения последовательности, необходимый для определения следующего ключа на авторизацию, а также время жизни ключа.

3. В процессе работы АС через промежуток времени, определяемый администратором системы, происходит повторная авторизация и аутентификация, и в случае успешного прохождения аутентификации и авторизации поток данных не прерывается.

В стандарте используется протокол PKM (Privacy Key Management), в соответствии с которым определено несколько видов ключей для шифрования передаваемой информации:

- Authorization Key (АК) — ключ, используемый для авторизации АК на базовой станции;
- Traffi c Encryption Key (ТЕК) — ключ, используемый для криптозащиты трафика;
- Key Encryption Key (КЕК) — ключ, используемый для криптозащиты передаваемых в эфире ключей.

Согласно стандарту, в каждый момент времени используются два ключа одновременно, с перекрывающимися временами жизни. Данная мера необходима в среде с потерями пакетов (а в эфире они неизбежны) и обеспечивает бесперебойность работы сети. Имеется большое количество динамически меняющихся ключей, достаточно длинных, при этом установление безопасных соединений происходит с помощью цифровой подписи. Согласно стандарту, криптозащита выполняется в соответствии с алгоритмом 3-DES, при этом отключить шифрование нельзя. Опционально предусмотрено шифрование по более надежному алгоритму AES

Практическая часть. Описание экспериментальной установки и методики измерений

Работа выполняется с использованием симулятора физического уровня стандарта IEEE 802.16-2004 в программной среде Simulink. Для запуска программы, в командную строку MATLAB необходимо ввести "commwman80216dstbc" и нажать Enter.

Схема исследуемой системы приведена на рисунке 7.75.

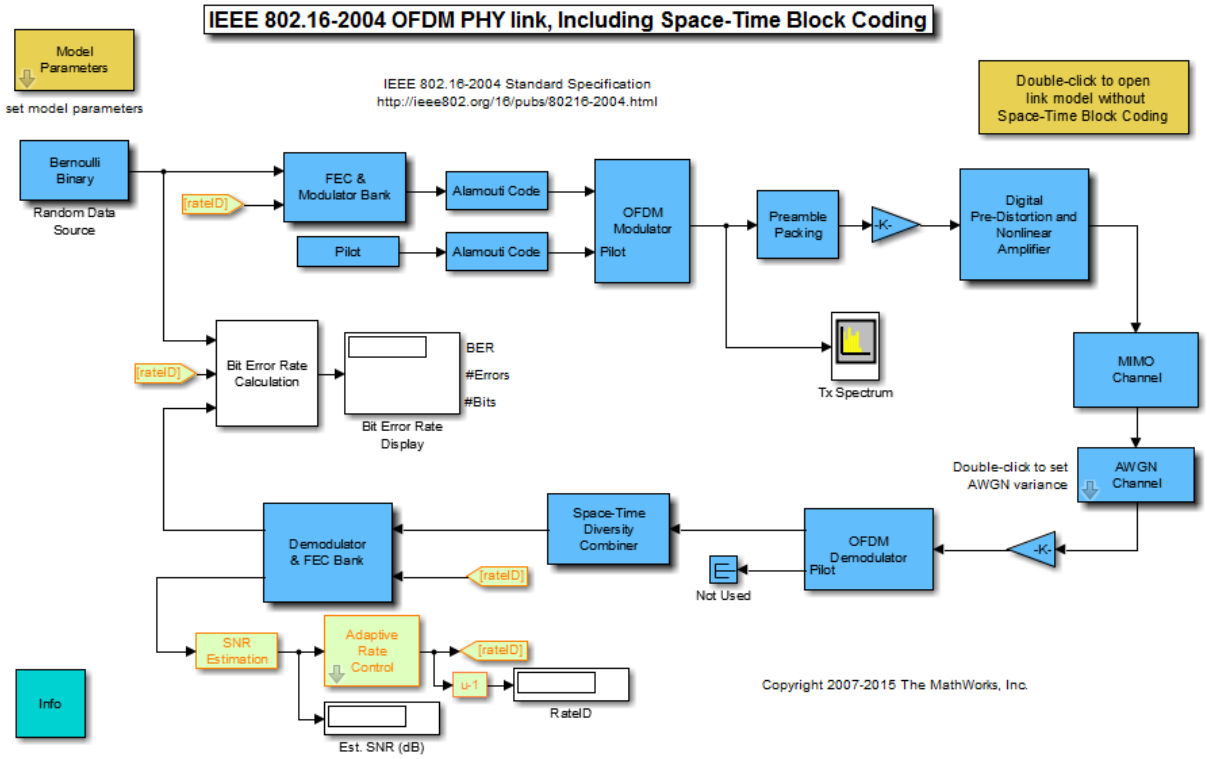


Рисунок 7.75 – Модель IEEE 802.16-2004 OFDM в MATLAB 2015b

Параметры источника случайной последовательности Bernulli Binary

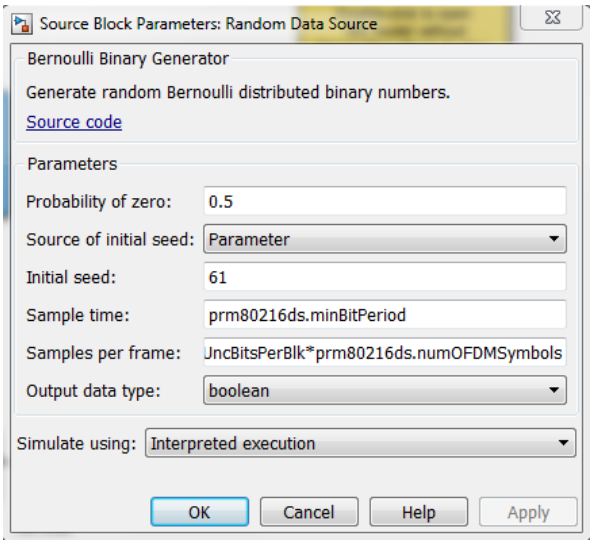


Рисунок 3.76 – Параметры блока Bernulli Binary

При проведении симуляции существует возможность изменения ряда параметров системы в следующих блоках:

Общие параметры модели (блок «Model Parameters», рисунок 7.77).

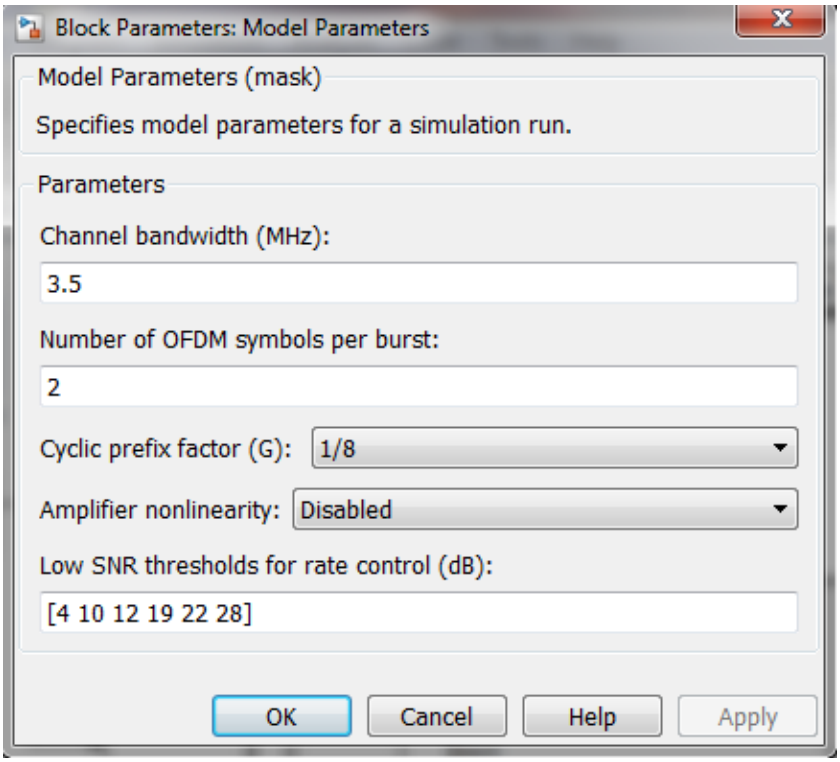


Рисунок 7.77 – Параметры системы, изменяемые в блоке «Model Parameters»

Блок помехоустойчивого кодирования и модуляции («FEC & Modulator Bank», рисунок 7.77) производит формирование сигнально-кодовой конструкции (СКК) определенного вида в зависимости от условий передачи.

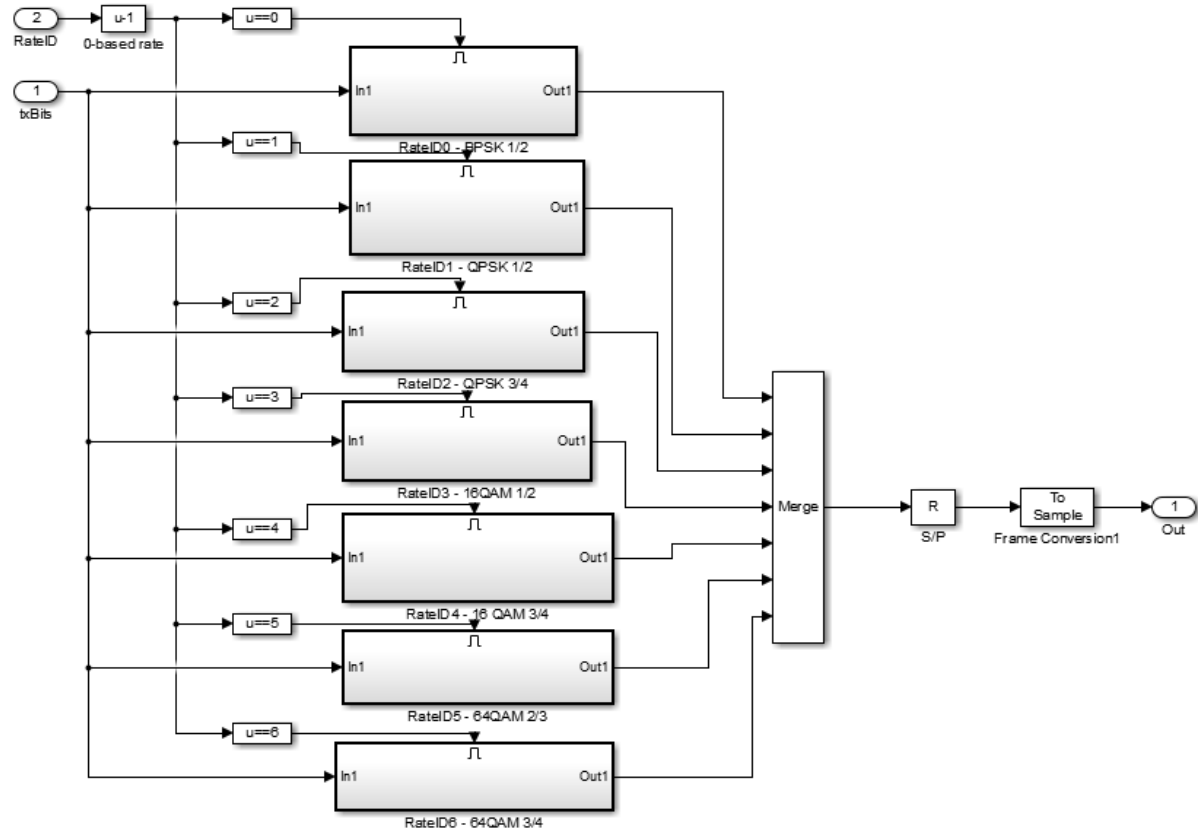


Рисунок 7.78 – Состав блока «FEC & Modulator Bank»

Рассмотрим состав каждого входящего блока:

Состав блока модулятора BPSK 1/2:

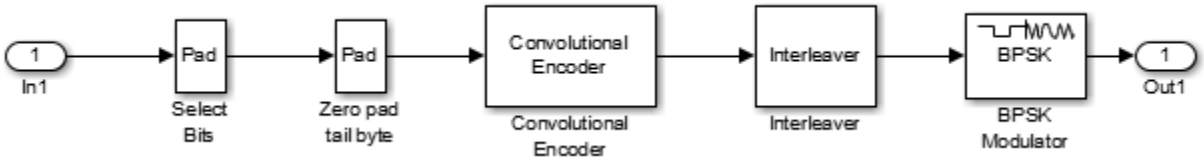


Рисунок 7.79 – Состав блока модулятора «BPSK 1/2»

Состав блока модулятора QPSK 1/2:

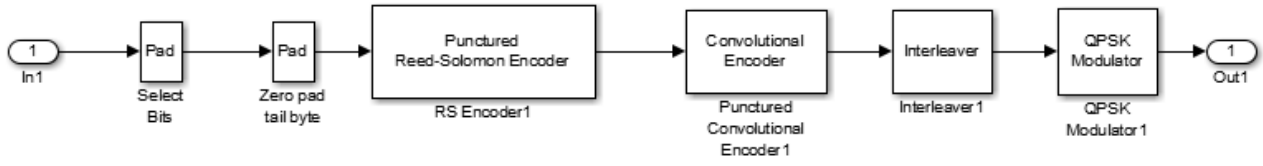


Рисунок 7.80 – Состав блока модулятора «QPSK 1/2»

Состав блока модулятора QPSK 3/4:

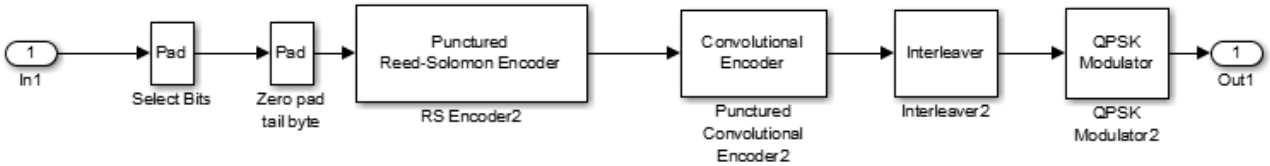


Рисунок 7.81 – Состав блока модулятора «QPSK 3/4»

Состав блока модулятора 16QAM 1/2:

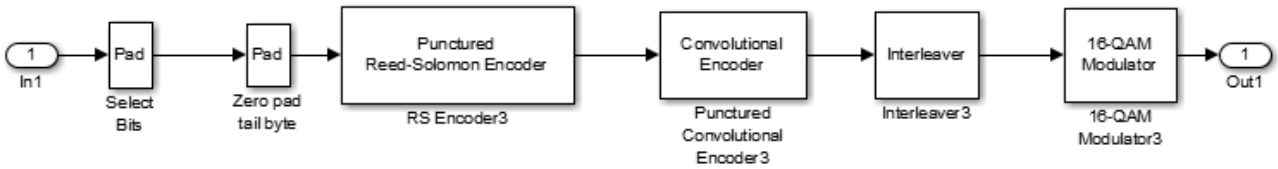


Рисунок 7.82 – Состав блока модулятора «16QAM 1/2»

Состав блока модулятора 16QAM 3/4:

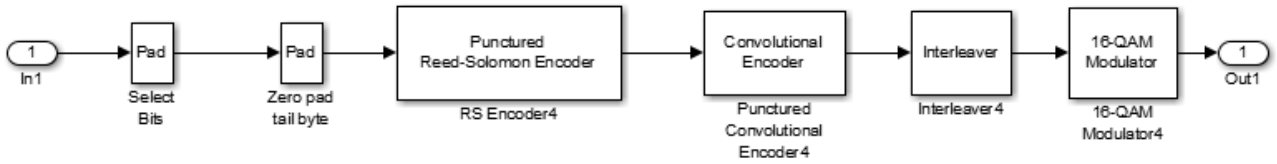


Рисунок 7.83 – Состав блока модулятора «16QAM 3/4»

Состав блока модулятора 64QAM 2/3:

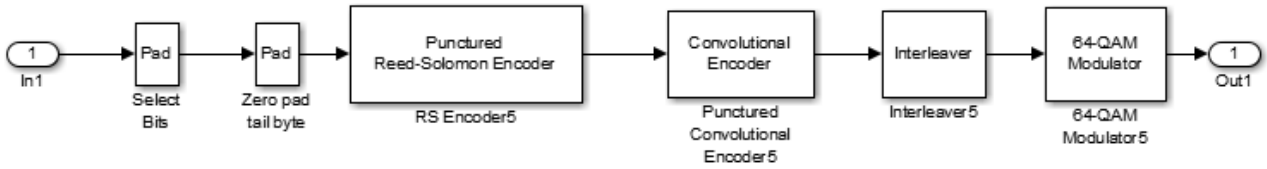


Рисунок 7.84 – Состав блока модулятора «64QAM 2/3»

Состав блока модулятора 64QAM 3/4:

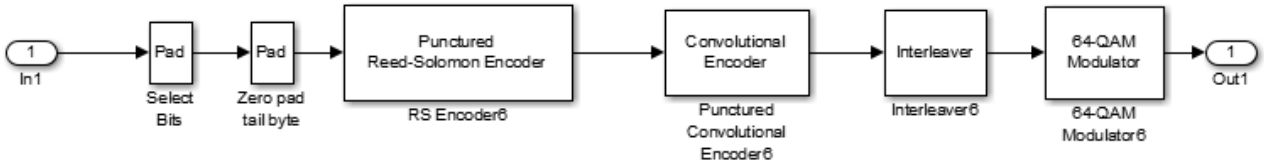


Рисунок 7.85 – Состав блока модулятора «64QAM 3/4»

Формирование сигнально-кодовых конструкций в каждом блоке происходит следующим образом: к поступающим информационным битам добавляется определяется «хвост» из нулевых бит, полученная последовательность кодируется блочным циклическим кодом Рида-Соломона. Следующий этап кодирования – сверточный код с использованием Треллис-структуры, затем, после перемежения, последовательность бит модулируется определенным образом для передачи по каналу.

В каждом из блоков на рисунках 7.79 – 7.85 используется одинаковая последовательность блоков, отличающихся своими параметрами. Например для блока «16QAM 1/2» блоки имеют параметры (рисунок 7.86 – 7.91).

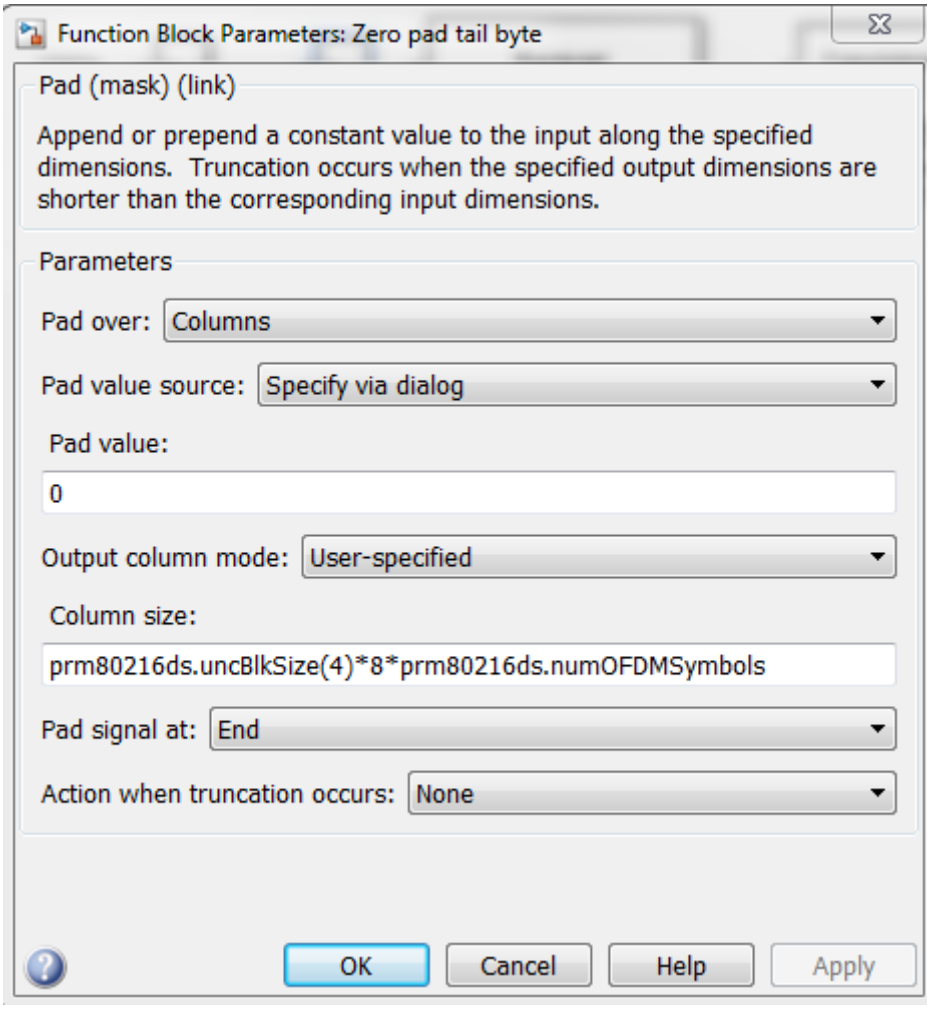


Рисунок 7.86 – Состав блока «Zero pad tail byte 16QAM 1/2»

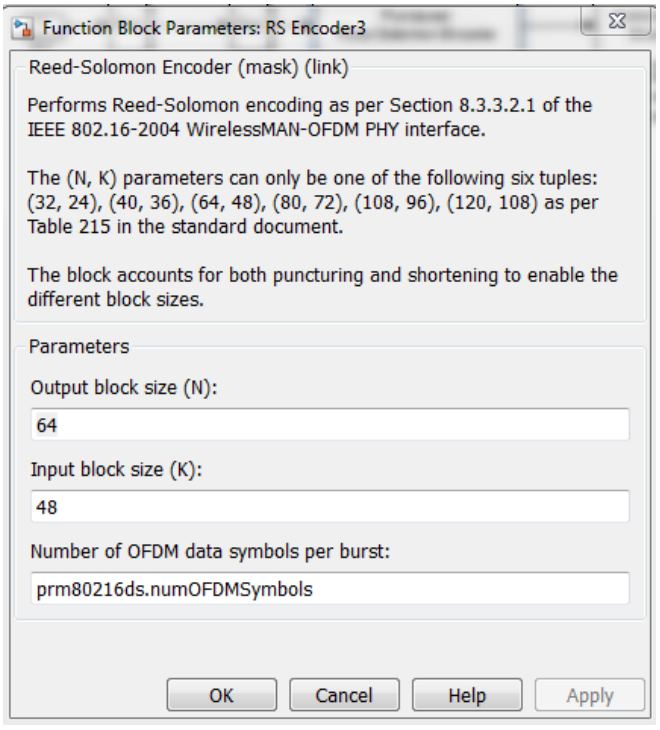


Рисунок 7.87 – Состав блока кодера Рида-Соломона «Puncured Reed-Solomon Encoder 16QAM 1/2»

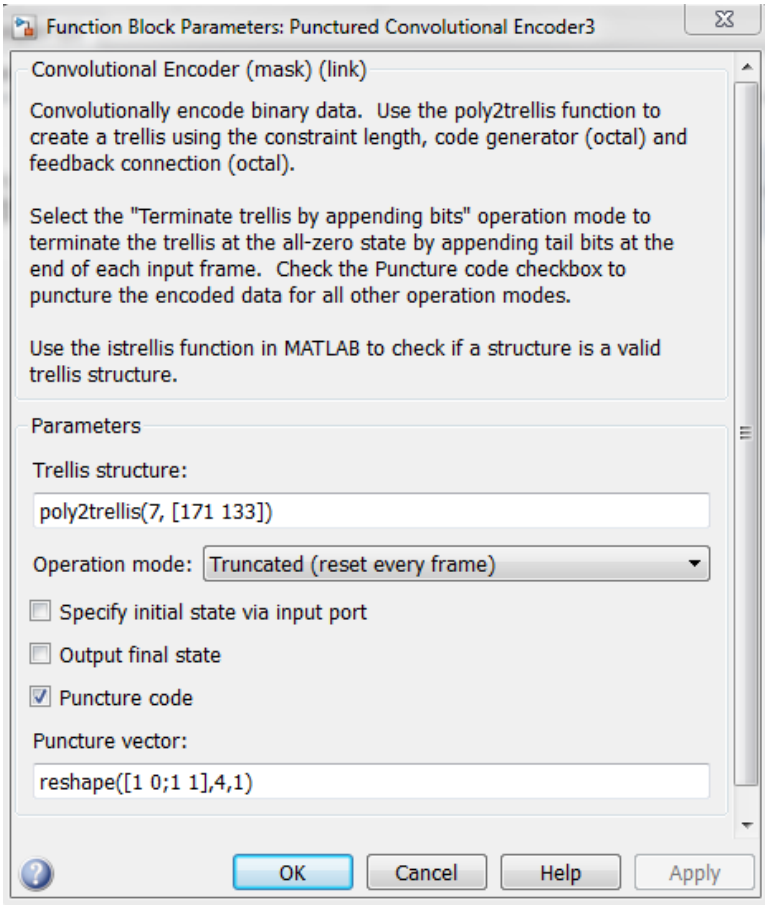


Рисунок 7.88 – Состав блока сверточного кодера«Convolutinal Encoder 16QAM 1/2»

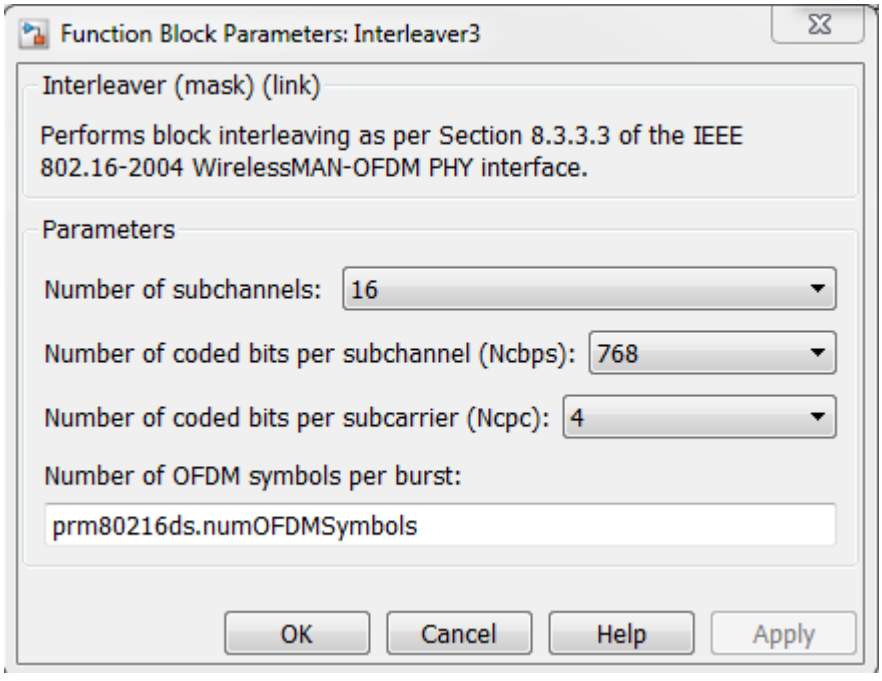


Рисунок 7.89 – Состав блока перемежителя «Interleaver 16QAM 1/2»

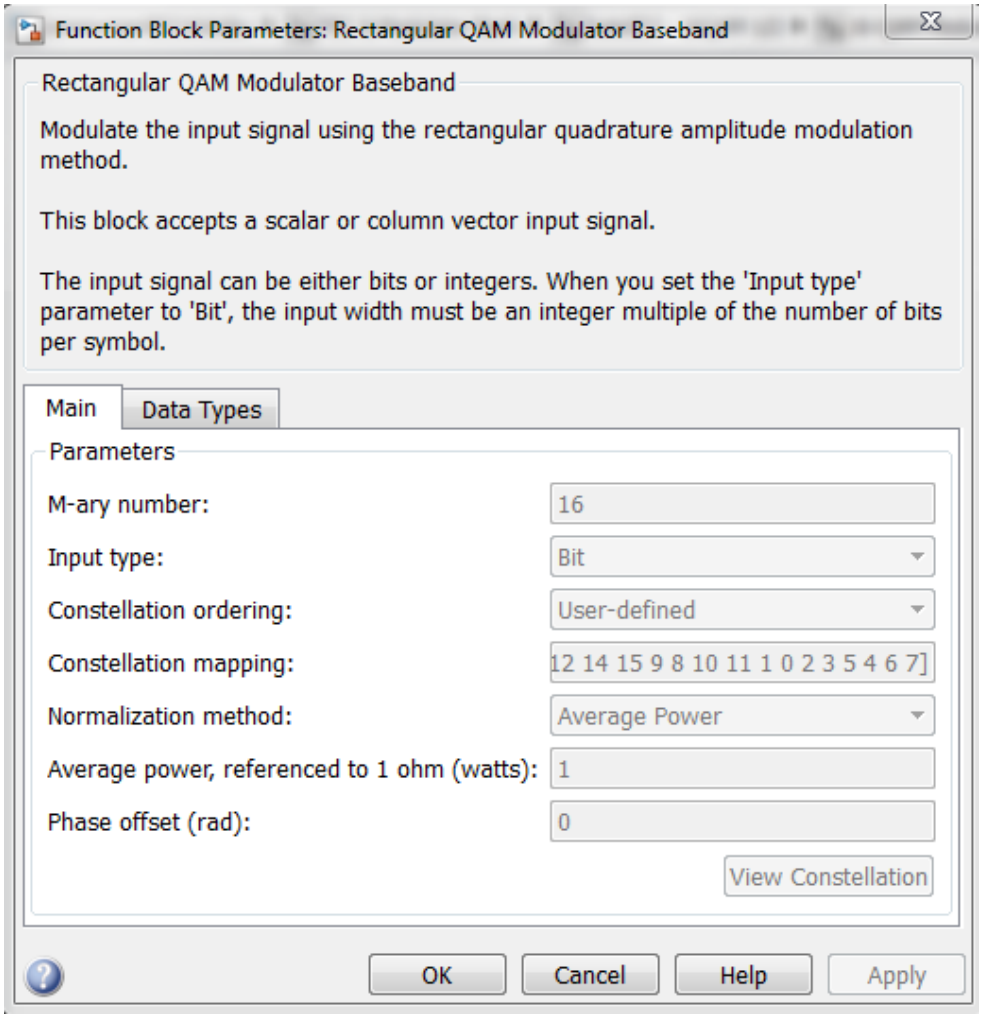


Рисунок 7.90 – Состав блока модулятора «16-QAM Modulator 16QAM 1/2»

Таблица 7.15 – Параметры кода Рида-Соломона для различных сигнально-кодовых конструкций

Вид модуляции	Общая скорость кодирования	Длина входной последовательности, бит	Длина выходной (кодированной) последовательности, бит	Параметры кода Рида-Соломона, (n, k, d)
BPSK	1/2	12	24	(12,12,0)
QPSK	1/2	24	48	(32,24,4)
QPSK	3/4	36	48	(40,36,2)
16-QAM	1/2	48	96	(64,48,8)
16-QAM	3/4	72	96	(80,70,4)
64-QAM	2/3	96	144	(108,96,6)
64-QAM	3/4	108	144	(120,108,6)

Состав блока помехоустойчивого декодирования и демодуляции («Demodulator & FEC Bank»)

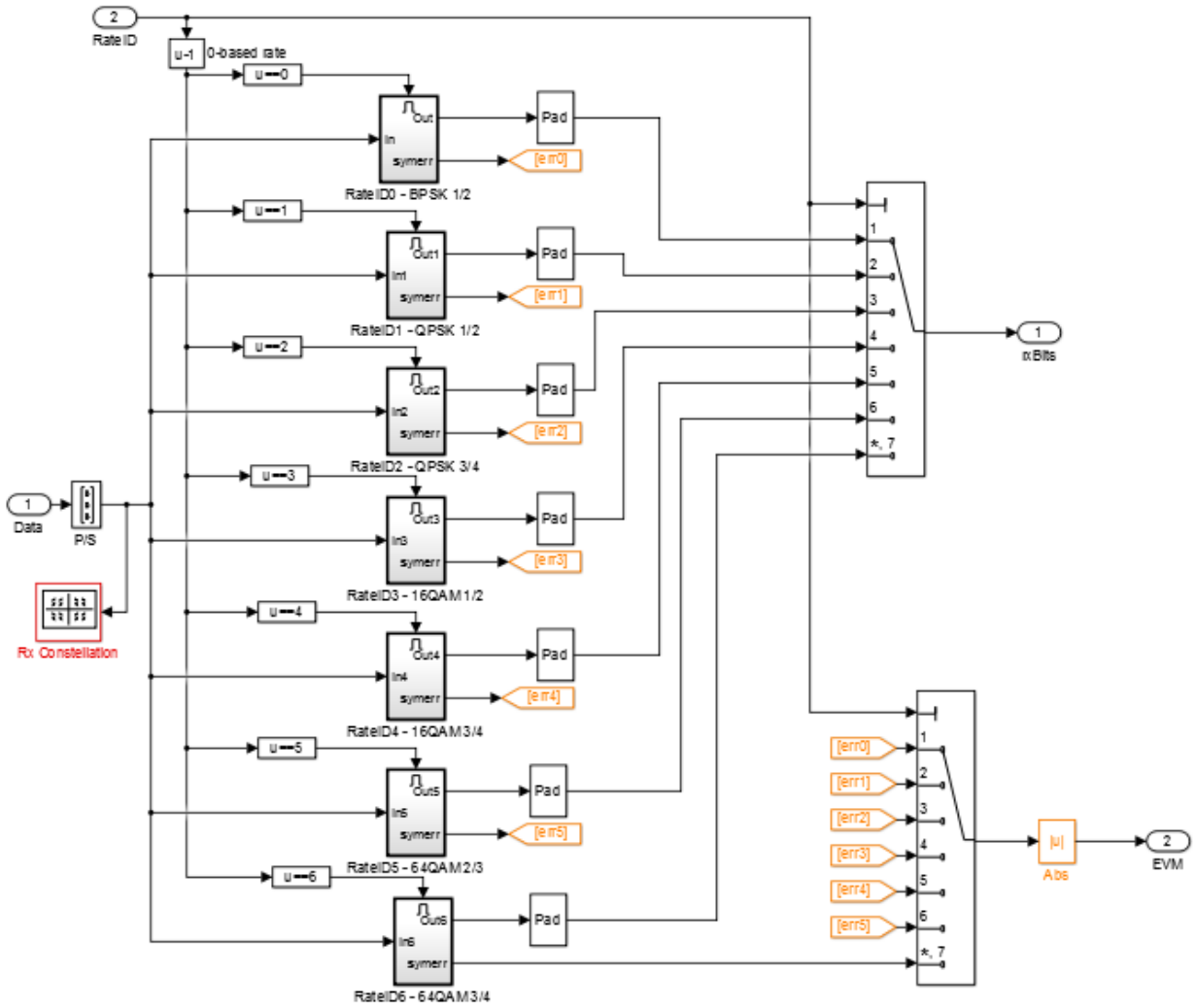


Рисунок 7.91 – Состав блока декодирования и демодуляции («Demodulator & FEC Bank»)

Состав блока BPSK 1/2 демодулятора

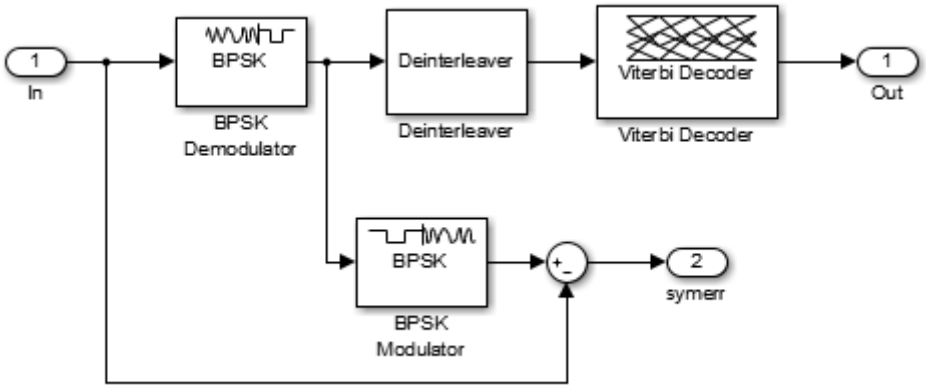


Рисунок 7.92 – Состав блока демодулятора «BPSK»

Состав блока QPSK 1/2 демодулятора

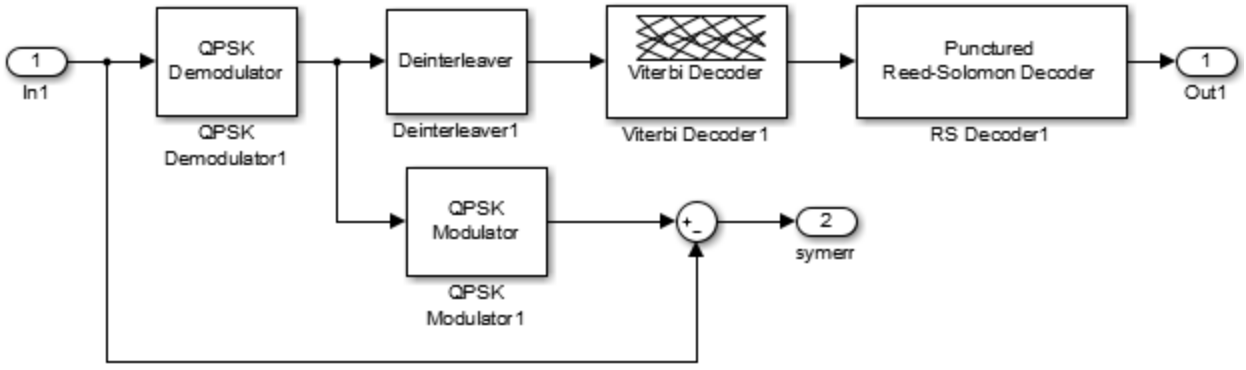


Рисунок 7.93 – Состав блока демодулятора «QPSK 1/2»

Состав блока QPSK 3/4 демодулятора

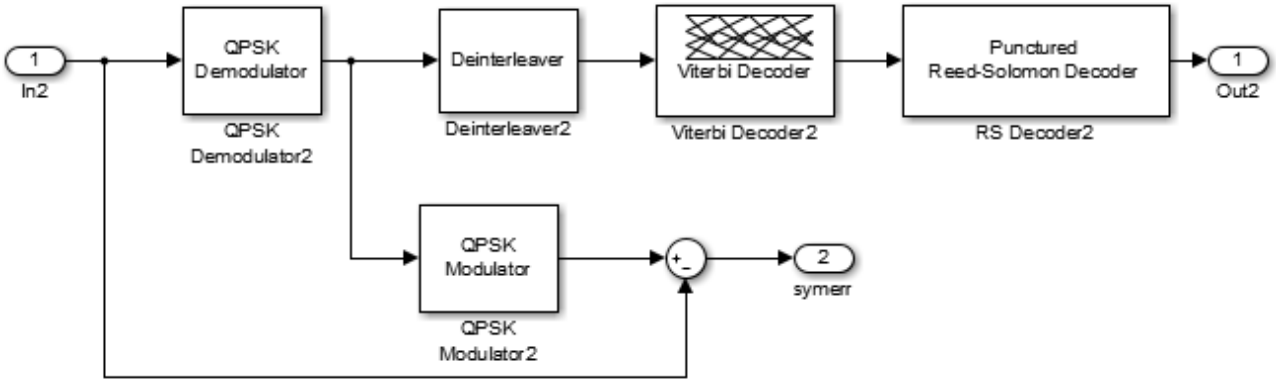


Рисунок 7.94 – Состав блока демодулятора «QPSK 3/4»

Состав блока 16QAM 1/2 демодулятора

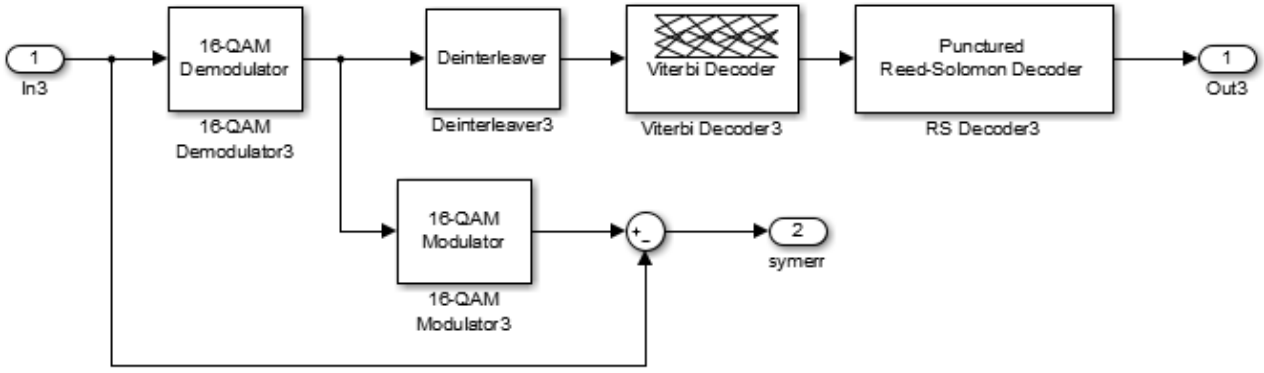


Рисунок 7.95 – Состав блока демодулятора «16QAM 1/2»

Состав блока 16QAM 3/4 демодулятора

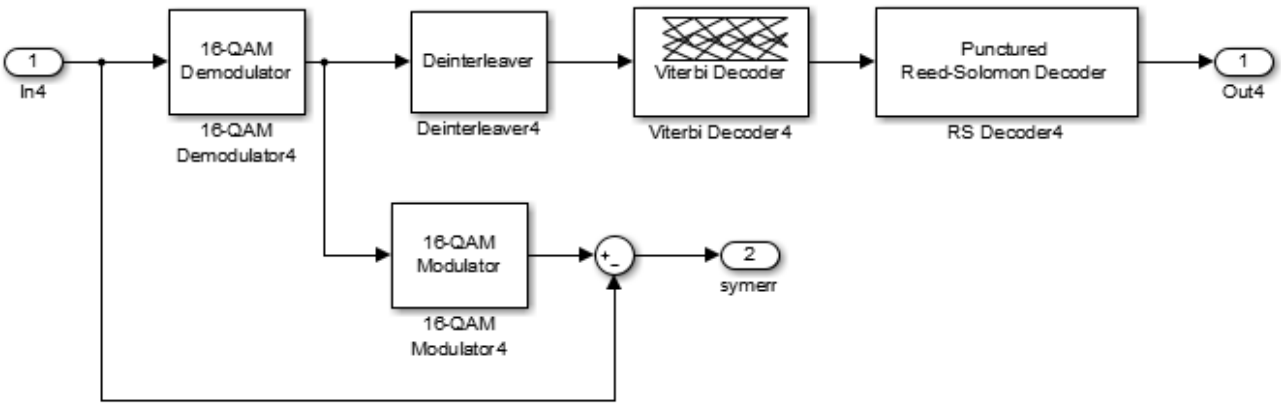


Рисунок 7.96 – Состав блока демодулятора «16QAM 3/4»

Состав блока 64QAM 2/3 демодулятора

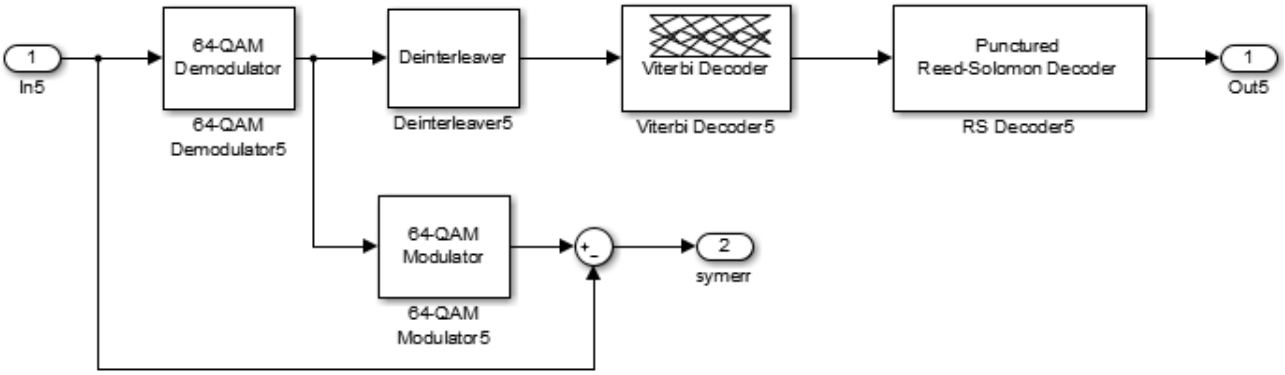


Рисунок 7.97 – Состав блока демодулятора «64QAM 2/3»

Состав блока 64QAM 3/4 демодулятора

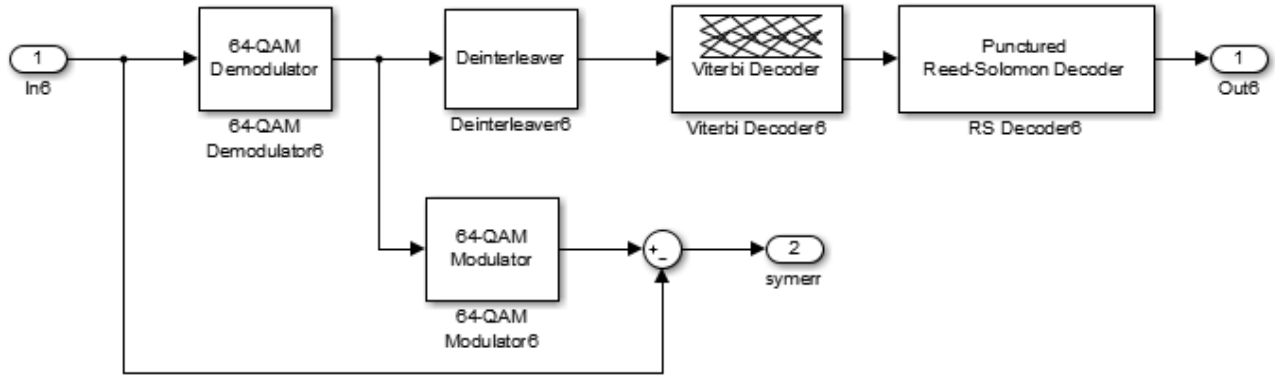


Рисунок 7.98 – Состав блока демодулятора «64QAM 3/4»

В процессе демодуляции и декодирования, описанные выше процессы, производятся в обратном порядке: демодуляция, деперемежение, декодирование сверточного кода по алгоритму Витерби, декодирования циклического блочного кода Рида-Соломона.

В каждом из блоков на рисунках 7.92 – 7.98 используется одинаковая последовательность блоков, отличающихся своими параметрами. Например для блока «16QAM 1/2» блоки имеют параметры (рисунок 7.99 – 7.103).

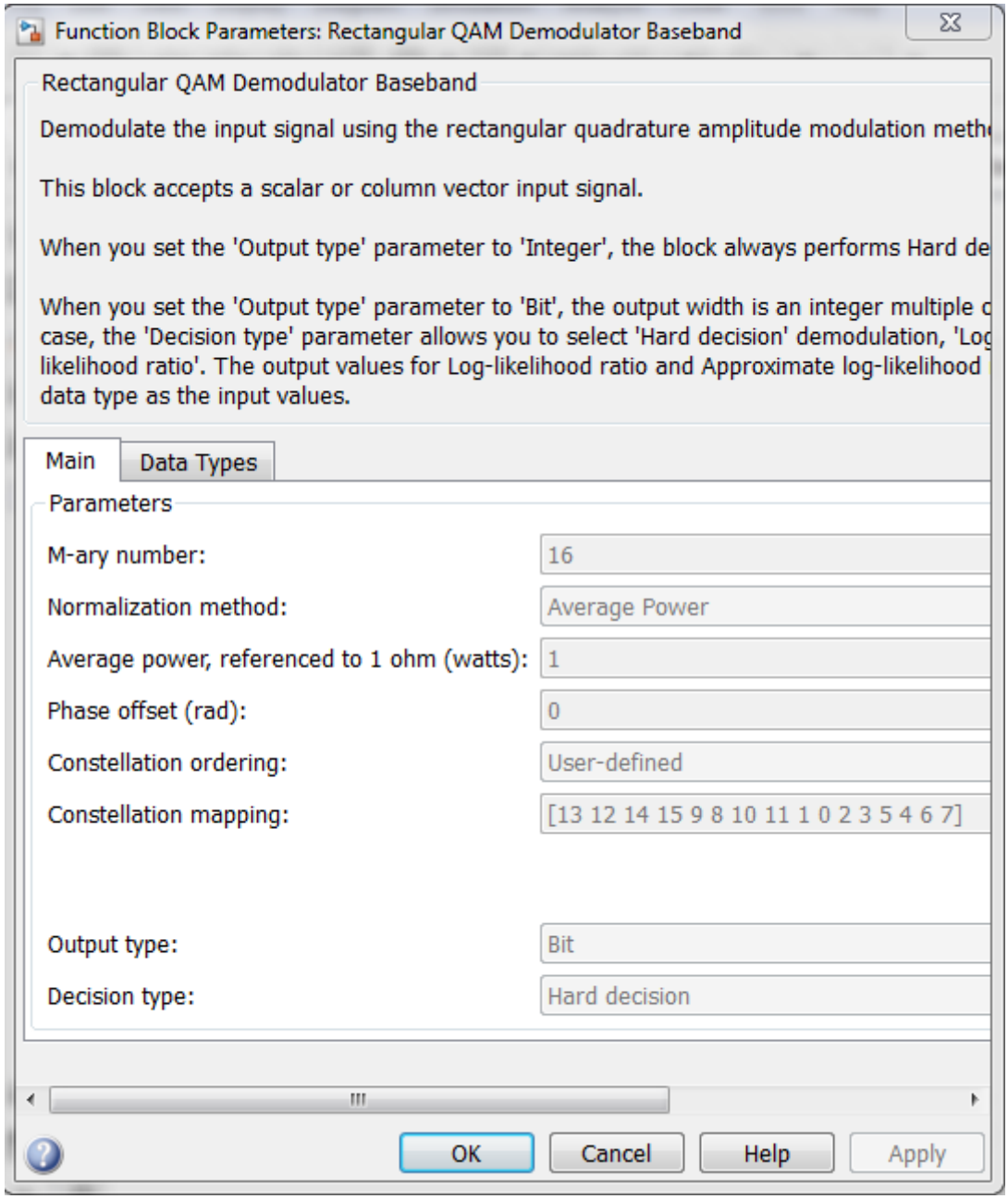


Рисунок 7.99 – Состав блока демодулятора «16-QAM Modulator 16QAM 1/2»

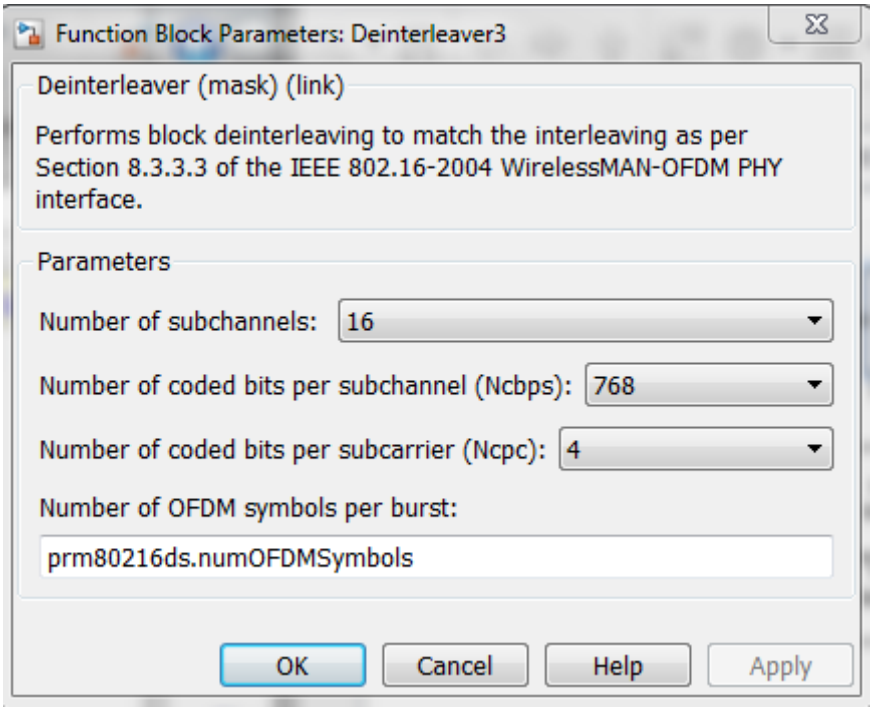


Рисунок 7.100 – Состав блока деперемежителя « Deinterleaver 16QAM 1/2»

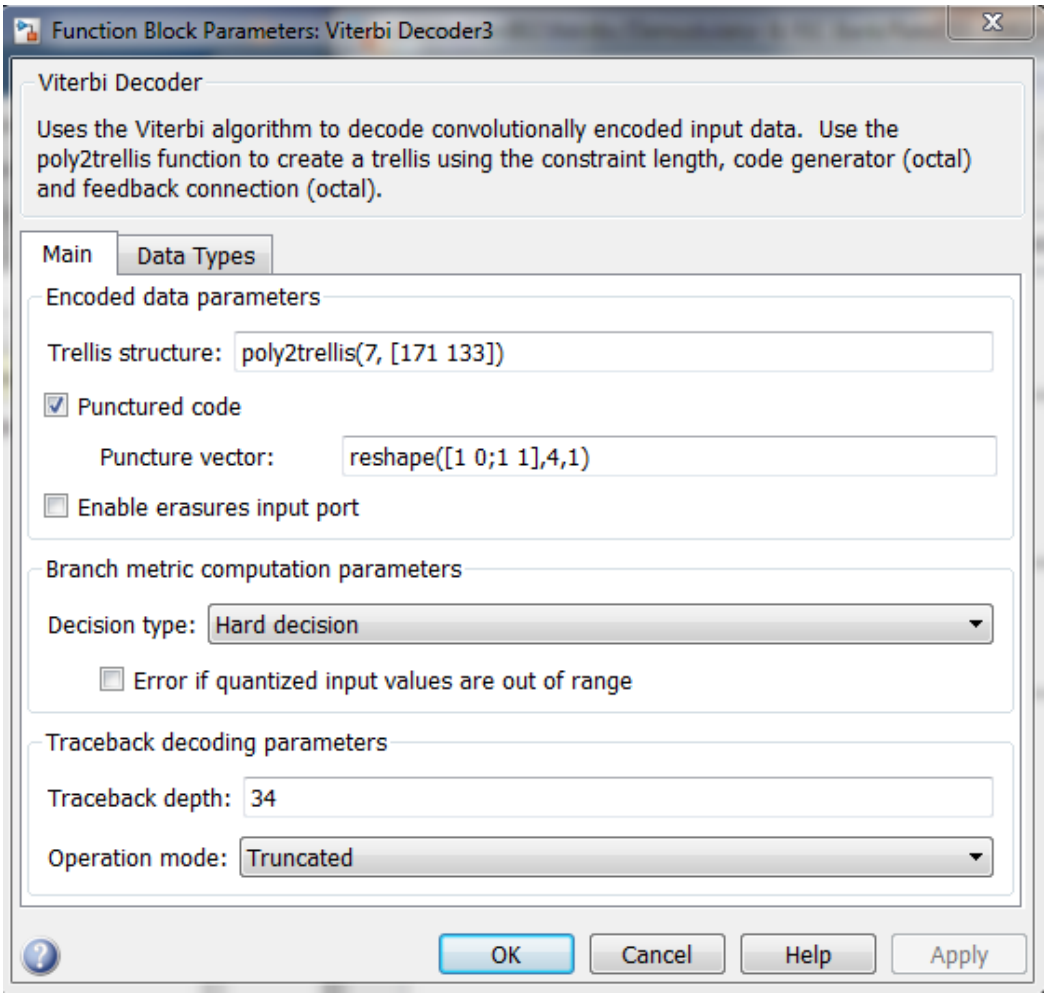


Рисунок 7.101 – Состав блока декодера Витерби «Viterbi Decoder 16QAM 1/2»

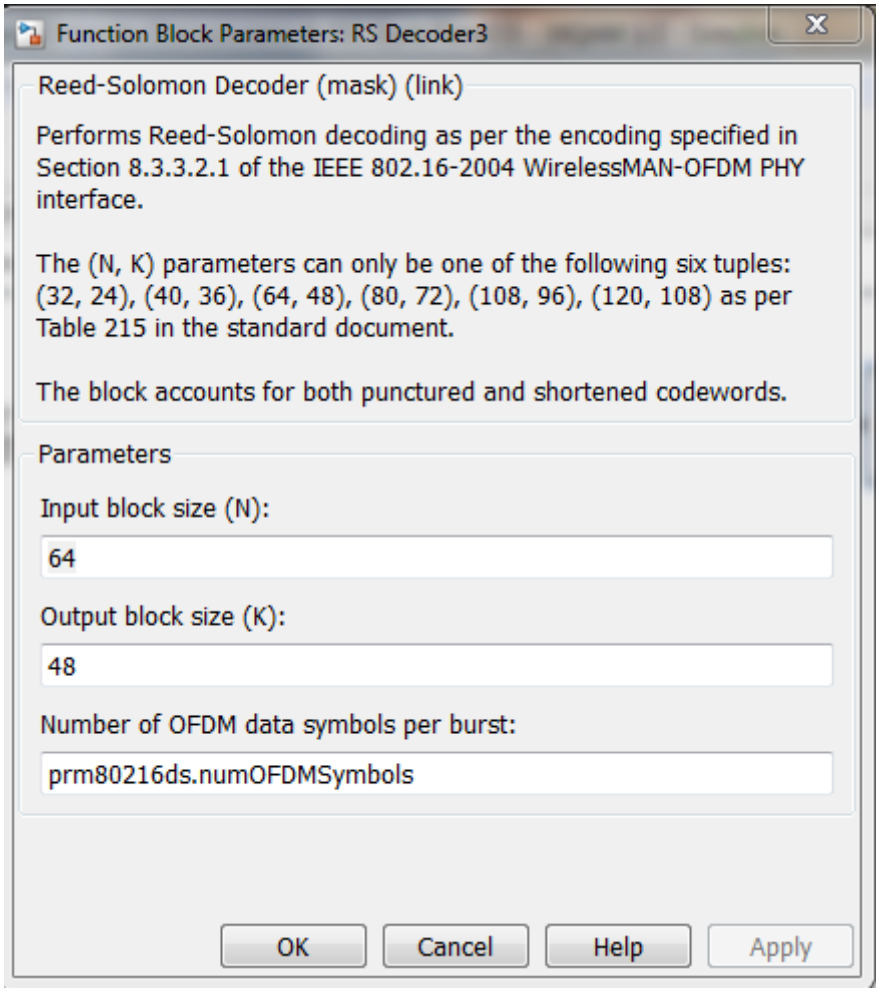


Рисунок 7.102 – Состав блока декодера Рида-Соломона «RS Decoder 16QAM 1/2»

В каждый момент времени, используемый вид модуляции и скорость кодирования (R) адаптируются под условия передачи. Блок «Adaptive Rate Control» анализирует уровень SNR в приемном устройстве и устанавливает параметры в соответствии с таблицей 3.2:

Таблица 7.16 – Изменение параметров модуляции и кодирования в зависимости от SNR

Вид модуляции и скорость кодирования	Отношение сигнал/шум в приемнике
BPSK	SNR < 4 дБ
QPSK, R=1/2	4 дБ < SNR < 10 дБ
QPSK, R=3/4	10 дБ < SNR < 12 дБ
16-QAM, R=1/2	12 дБ < SNR < 19 дБ
16-QAM, R=3/4	19 дБ < SNR < 22 дБ
64-QAM, R=1/2	22 дБ < SNR < 28 дБ
64-QAM, R=3/4	SNR > 28 дБ

Параметры OFDM-модулятора (блок «OFDM Modulator», рисунок 7.103).

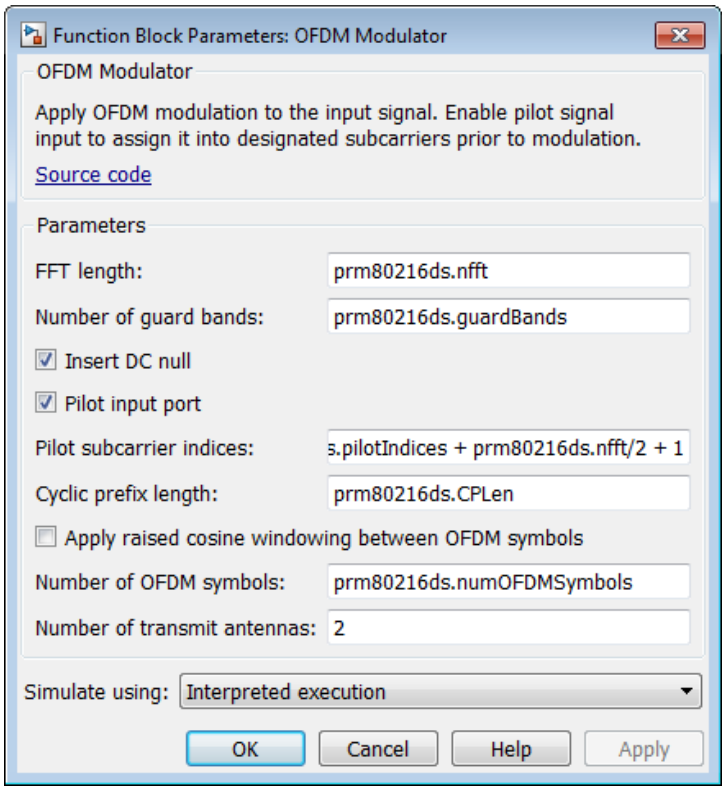


Рисунок 7.104 – Параметры системы, изменяемые в блоке «OFDM Modulator»

Параметры OFDM-демодулятора (блок «OFDM Demodulator», рисунок 7.105).

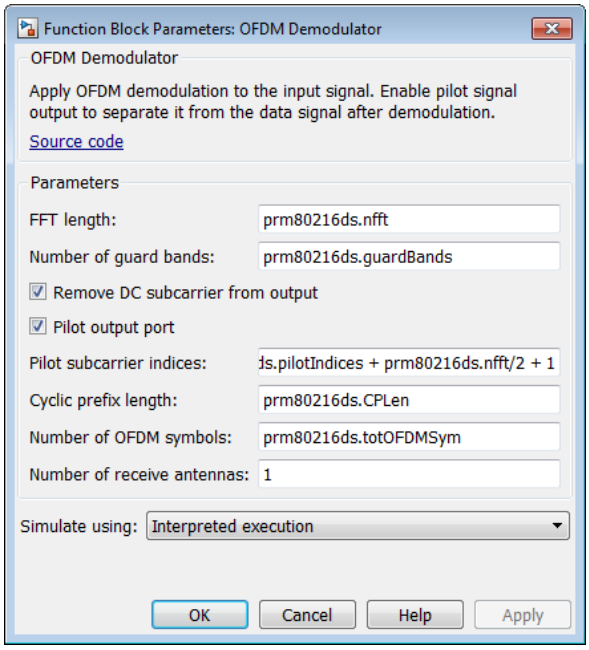


Рисунок 7.105 – Параметры системы, изменяемые в блоке «OFDM Demodulator»

Параметры канала MIMO (блок «MIMO Channel», рисунок 3.31).

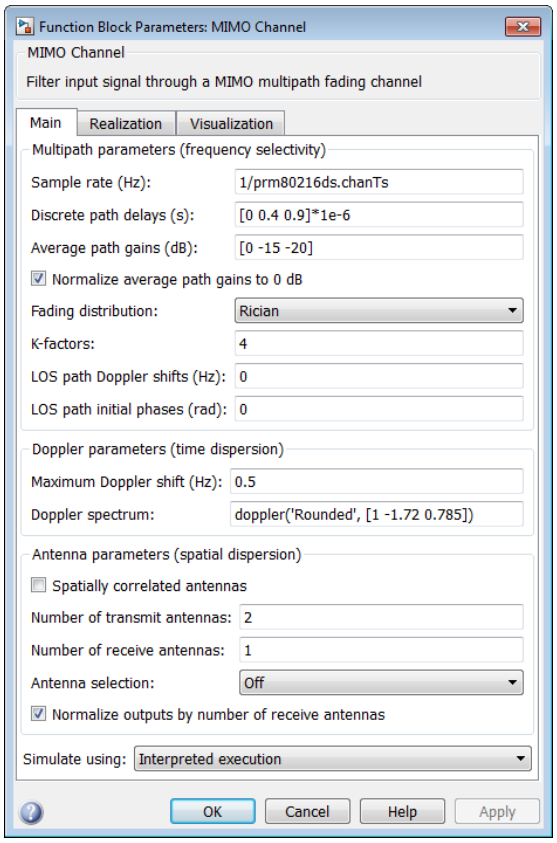


Рисунок 7.106 – Параметры системы, изменяемые в блоке «MIMO Channel»

Параметры канала AWGN (блок «AWGN Channel», рисунок 3.32).

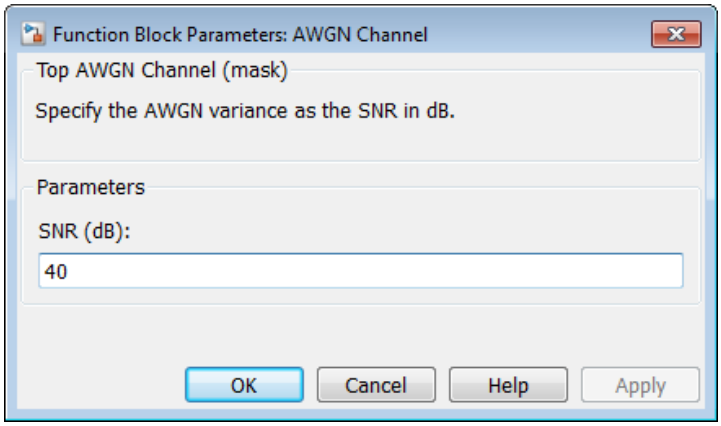


Рисунок 7.107 – Параметры системы, изменяемые в блоке «AWGN Channel»

Результаты работы и их анализ

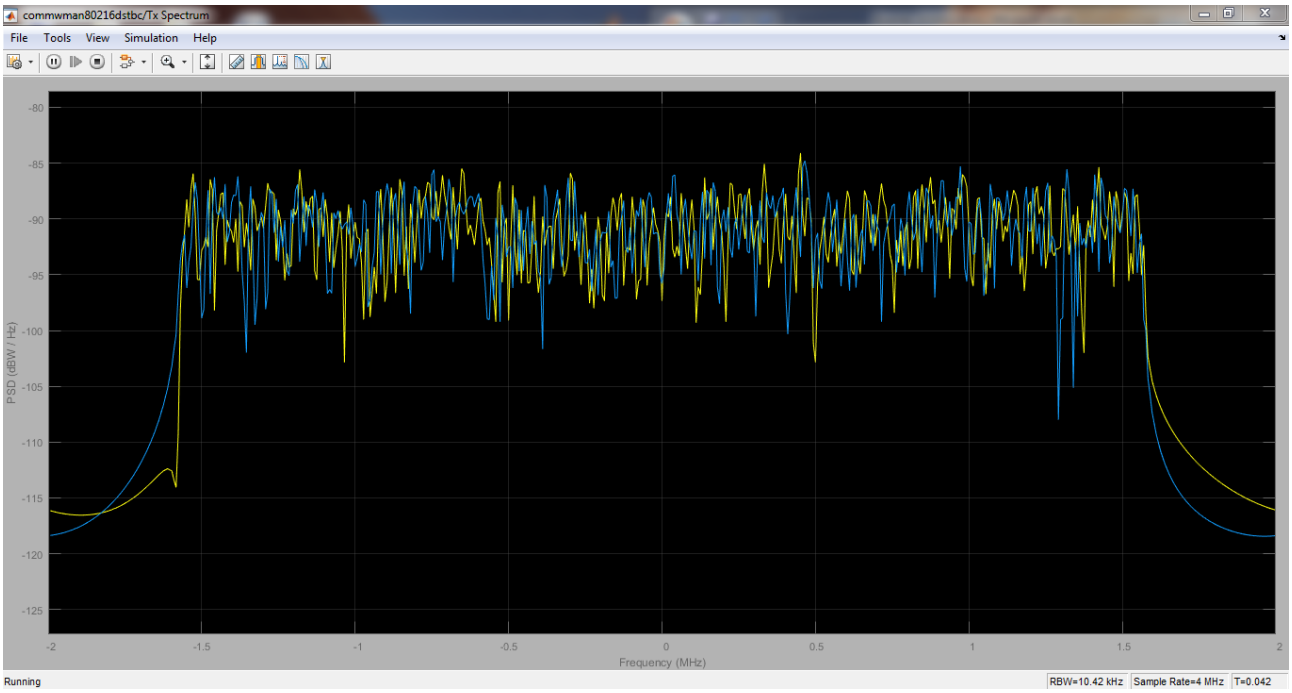


Рисунок 7.108 – Спектр передаваемых сигналов, поступающих на соответствующую передающую антенну

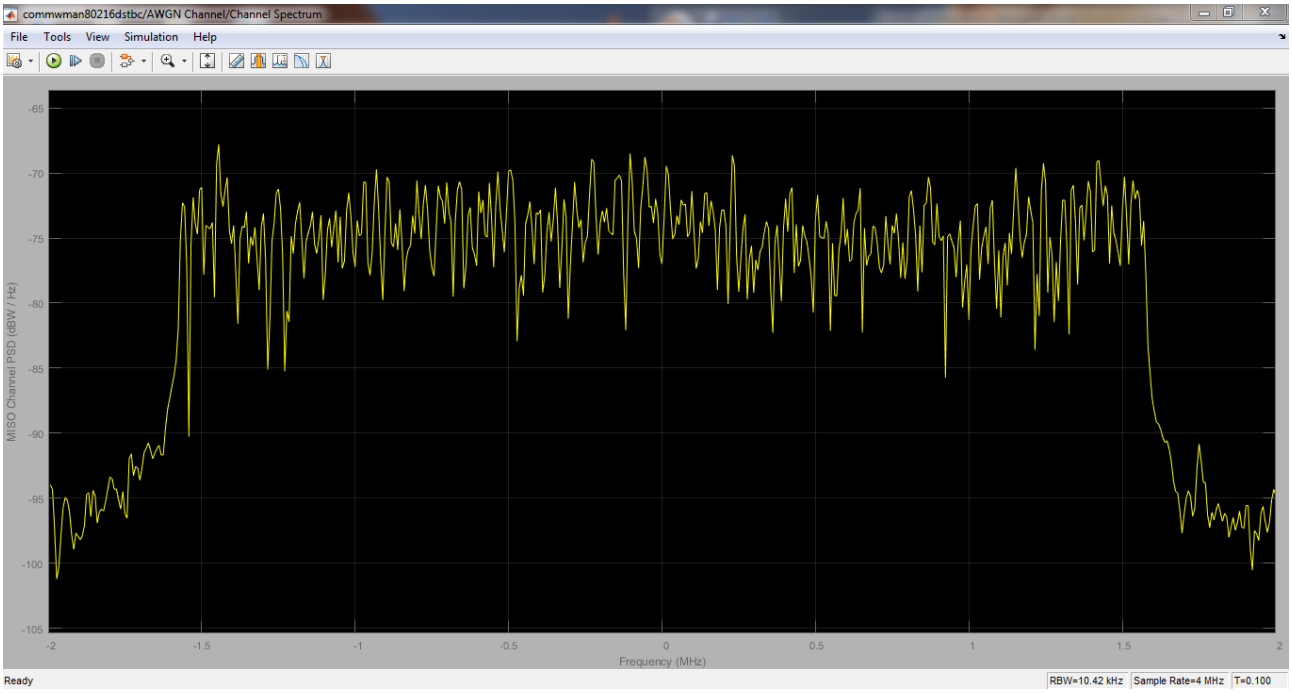


Рисунок 7.109 – Спектр принимаемого сигнала

Как было описано ранее, система адаптируется к условиям передачи, изменяя вид сигнально-кодовой конструкции сигнала (таблица 3.16). Необходимо исследовать поведение системы в зависимости от SNR в канале передачи (блок AWGN Channel), оформить полученные значения в виде графиков.

Созвездие принимаемого сигнала (BPSK):

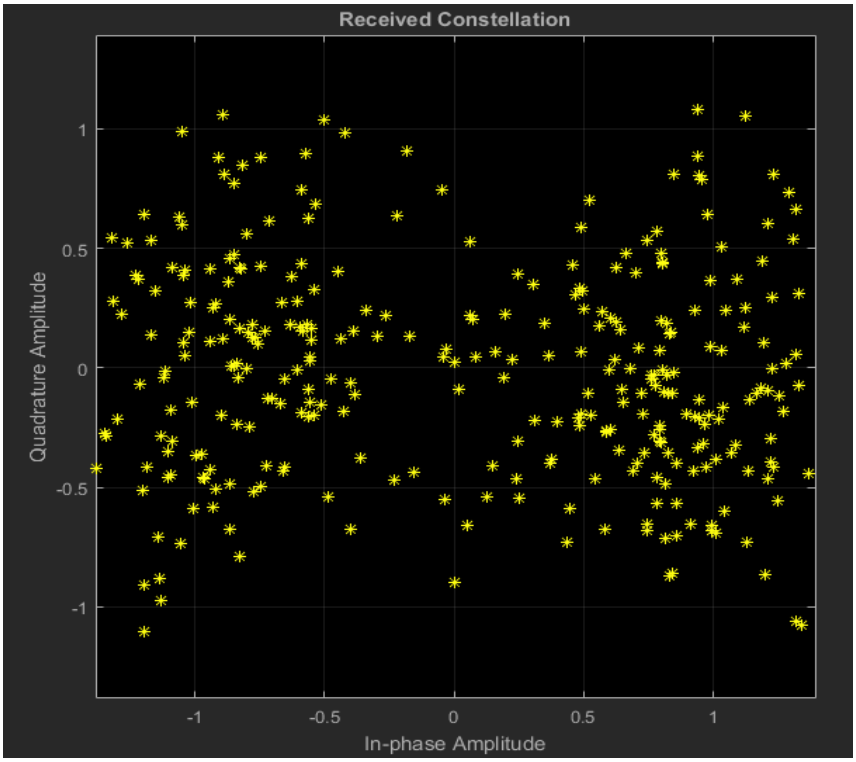


Рисунок 7.110 – Созвездие принимаемого сигнала (SNR = 2)

Созвездие принимаемого сигнала (QAM-4):

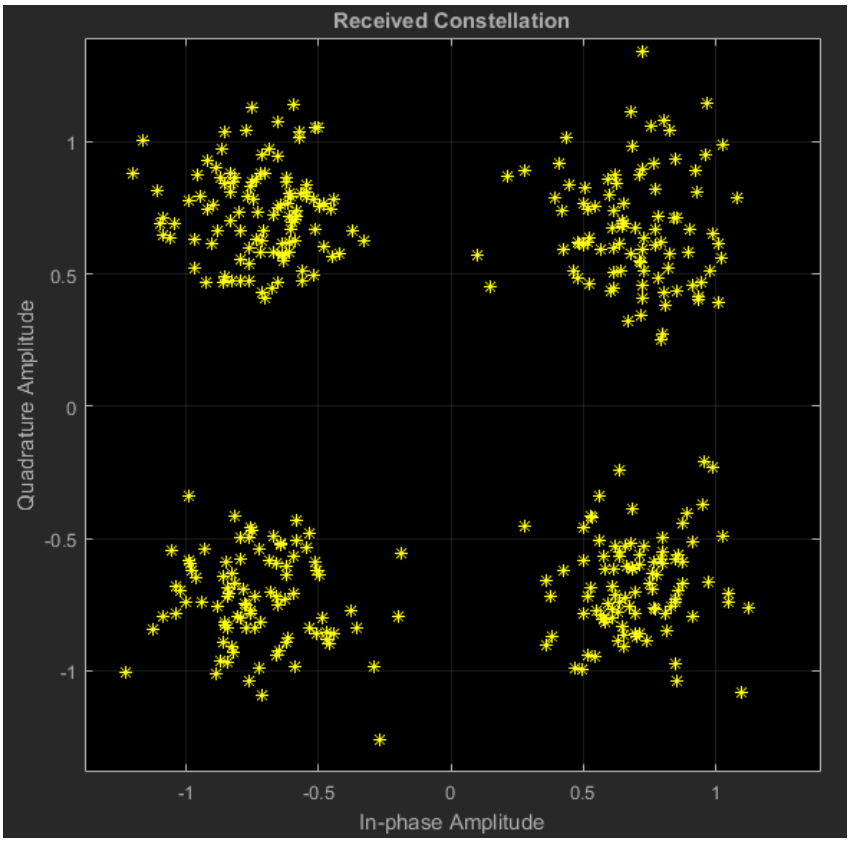


Рисунок 7.111 – Созвездие принимаемого сигнала (SNR = 11)

Созвездие принимаемого сигнала (QAM-16):

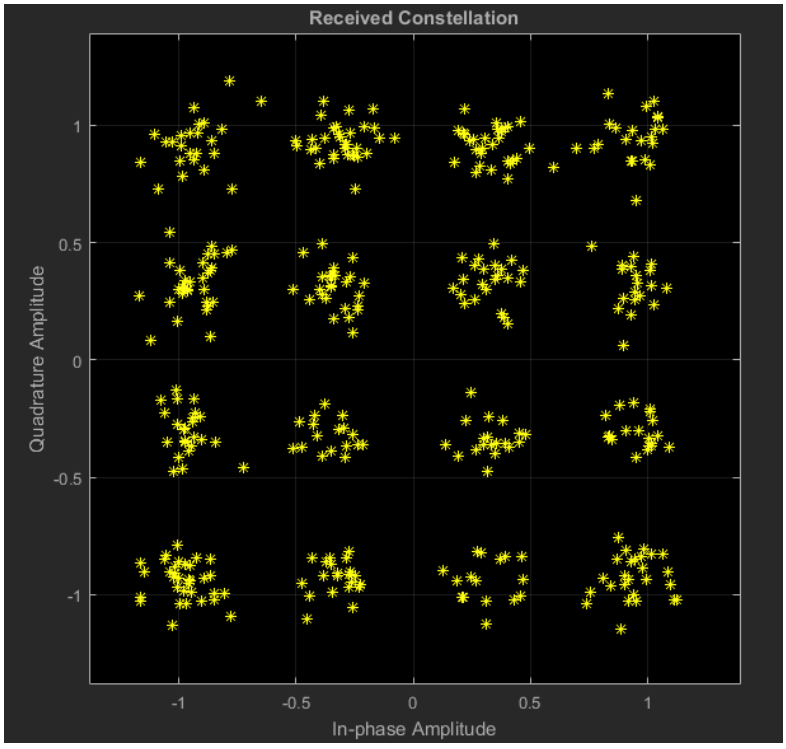


Рисунок 7.112 – Созвездие принимаемого сигнала (SNR = 18)

Созвездие принимаемого сигнала (QAM-64):

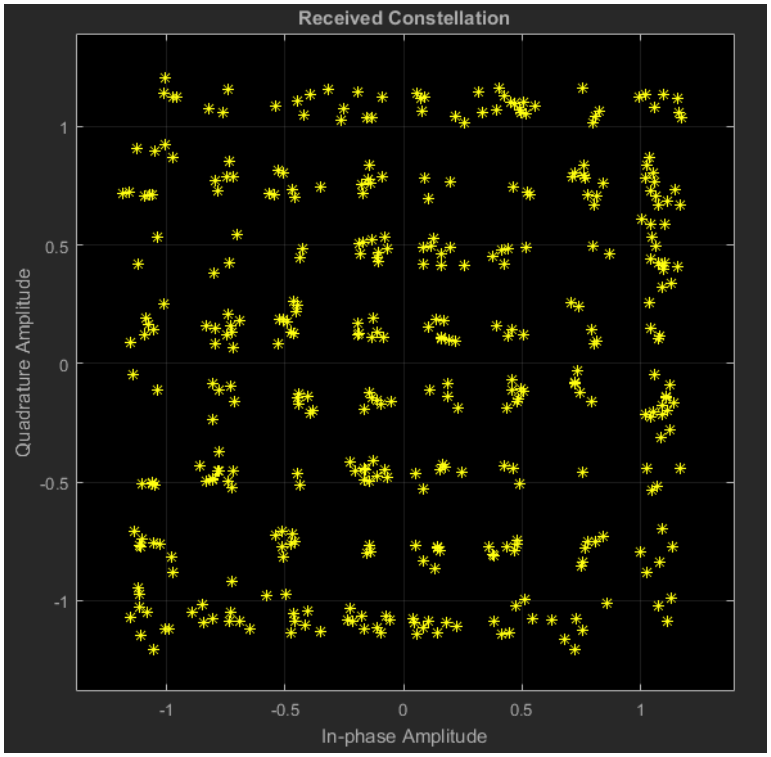


Рисунок 3.113 – Созвездие принимаемого сигнала (SNR = 22)

По данным блока «Bit Error Rate Display» можно построить график зависимости битовой вероятности ошибки (BER) от отношения сигнал/шум в канале (рисунок 3.38).

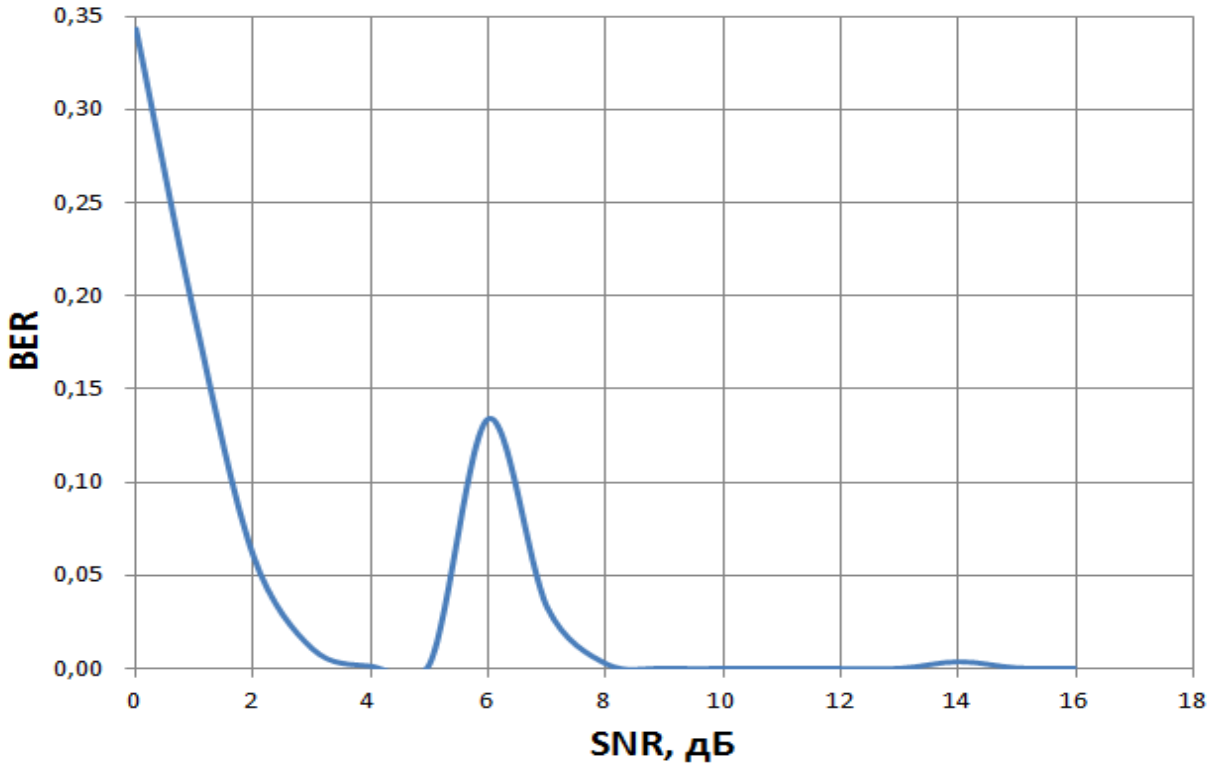


Рисунок 7.114 – Зависимость BER от SNR при использовании адаптивного изменения параметров.

Зависимости BER от SNR для каждого конкретного вида модуляции и скорости кодирования представлены на рисунке 3.39

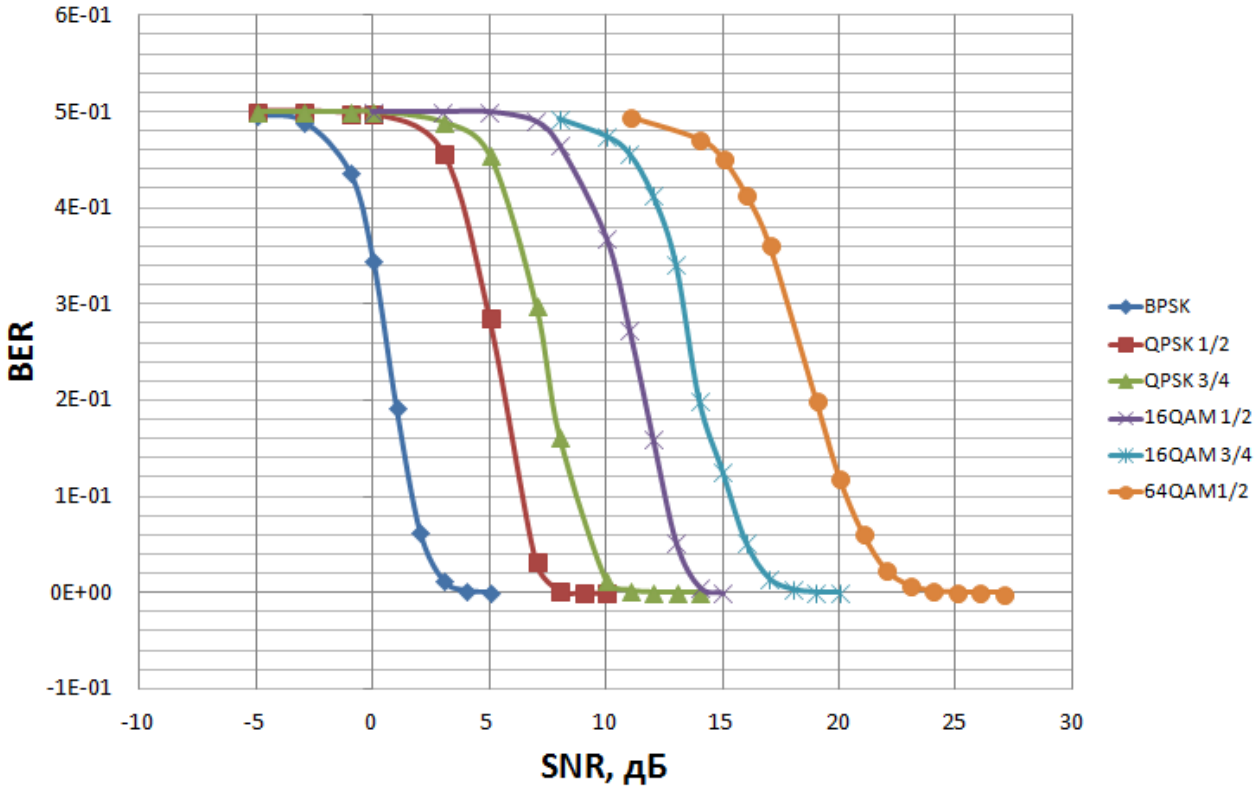


Рисунок 7.115 – Графики зависимости BER от SNR для отдельных видов модуляции и скорости кодирования.

Та же зависимость в логарифмическом масштабе:

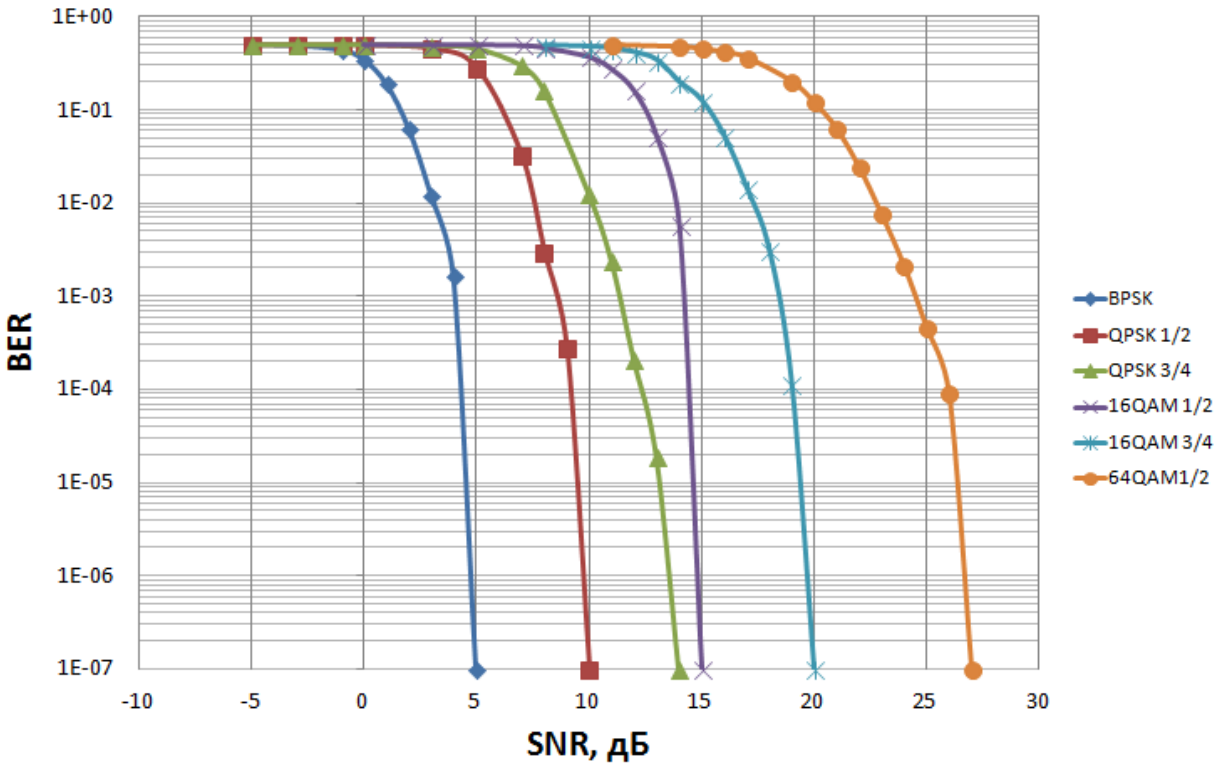


Рисунок 7.115 – Графики зависимости BER от SNR для отдельных видов модуляции и скорости кодирования. Логарифмическая шкала

Переход с одного вида модуляции на другой требует большей энергетики сигнала, но взамен происходит значительное увеличение скорости передачи. На рисунке 7.116 представлена зависимость принятого количества бит за 1 секунду (скорость передачи в Мбит/с) от SNR в канале.

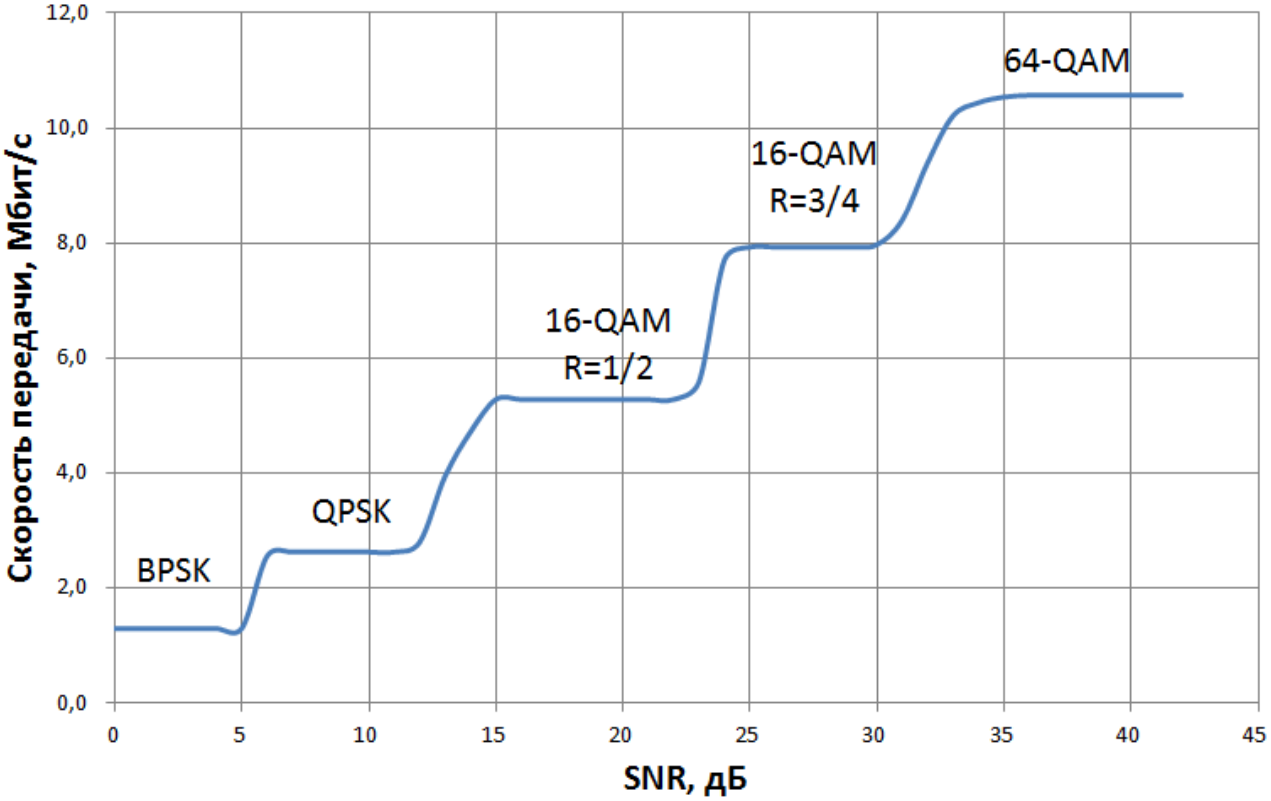


Рисунок 7.116 – График зависимости скорости передачи от SNR

После демодуляции и декодирования производится оценка SNR для принятых данных (блок «SNR Estimation»). Зависимость оцененного SNR от SNR в канале передачи приведена на рисунке 7.117

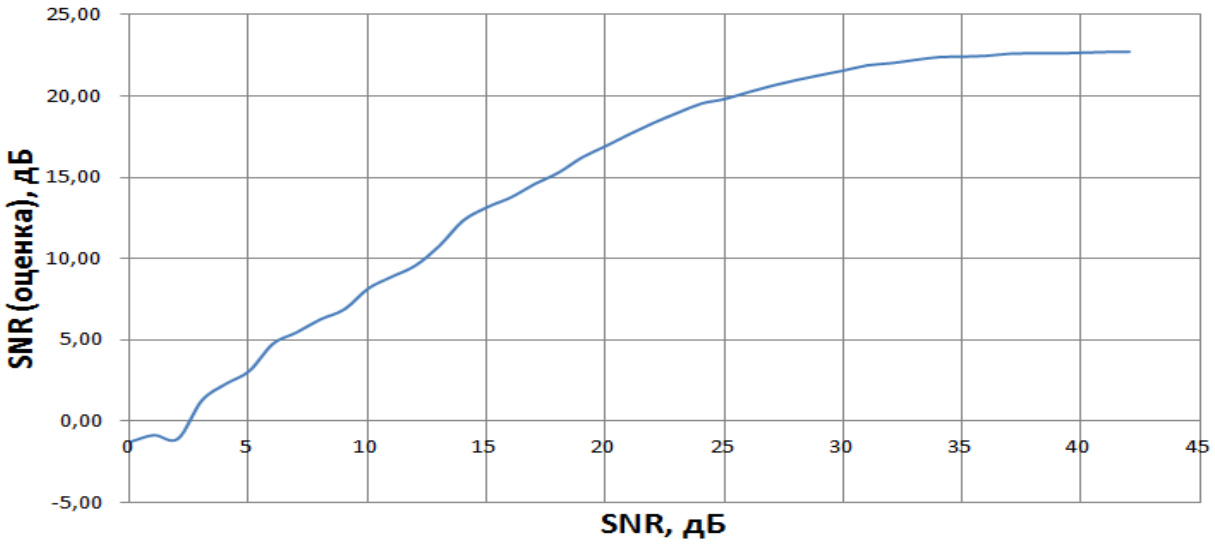


Рисунок 7.117 – График зависимости оценки SNR от SNR в канале передачи

В результате проделанной работы были получены теоретические знания об основах построения беспроводных сетей WiMAX на основе протокола IEEE 802.16-2004. Изучены сетевой, канальный и физический уровни данного протокола.

По результатам практического исследования модели физического уровня IEEE 802.16-2004 были сделаны следующие выводы:

1. Сравнивая рисунки 3.38 и 3.39 видно, что адаптивное изменение параметров системы в зависимости от SNR в канале приводит к уменьшению вероятности ошибок. Выбросы значений BER при SNR = 6 и 14 дБ происходят из-за перехода на менее помехозащищенные, но более скоростные виды модуляции.

2. Одновременно с этим происходит увеличение скорости передачи (рисунок 3.41). Скорость передачи изменяется от 1.25 Мбит/с при использовании BPSK до 11 Мбит/с при использовании 64-QAM.

3. По графику зависимости оценки SNR от реального SNR (рисунок 3.42), можно сделать вывод, что система работает наиболее стабильно (зависимость линейна) на участке 5…24 дБ. При SNR > 24 дБ более точная оценка канала не требуется (выбирается наименее помехоустойчивый метод модуляции – QAM-64 (в рамках стандарта)). При SNR < 6 дБ выбирается наиболее помехоустойчивый метод модуляции – BPSK.

7.7. Проектирование защищенной системы мобильной связи стандарта IEEE 802. 20 (LTE) на базе ПО MATLAB

Целью раздела является приобретение и закрепление навыков организации и реализации в программной среде системы мобильной связи стандарта LTE, подробное изучение схем входящих в состав стандарта и программного обеспечения с которыми предстоит работать при выполнении курсового проекта, умения выбрать необходимые решения на основе требований технического задания.

Помимо теоритической части, задачей курсового проектирования является построение в программной среде схемы передачи информации от базовой станции (БС) к мобильной станции (МС) и ее анализ. Схема будет включать в свой состав: генератор бинарной последовательности, кодек, модулятор/демодулятор, канал связи, анализатор ошибок и т.д.

Основным отличием стандарта LTE от предыдущих стандартов сетей связи является применение «плоской» более упрощённой IP-архитектуры, которая способствует уменьшению задержек при установленной Интернет-сессии. В стандарте LTE использовано два принципиально новых метода увеличения пропускной способности. Первый заключается в применении технологии MIMO (Multiple Input Multiple Output), где передача и приём

сигнала осуществляется одновременно через несколько передающих и приёмных антенн. Таким образом, повышается скорость передачи данных в беспроводных сетях. Второй метод заключается в применении OFDM (Orthogonal frequency division multiplexing) модуляции, использующей несколько поднесущих. Преимущество данного метода заключается также в том, что системы связи с LTE могут работать в отсутствии прямой видимости.

Стандарты 2G и 3G

Стандарт 2G (GSM)

Разработка стандарта GSM началась еще в 1982 году организацией по стандартизации CEPT (European Conference of Postal and Telecommunications Administrations) . В 1991 году в Финляндии была введена в эксплуатацию первая в мире сеть GSM. Уже к концу 1993 года число абонентов, использующих этот стандарт, перевалило за миллион. К этому времени сети GSM были развернуты в 73 странах мира.

Сети стандарта GSM позволяют предоставлять широкий перечень услуг:

- Голосовые соединения
- Услуги передачи данных (до 384 кбит/сек благодаря технологии EDGE (дополнение технологии GPRS, в результате появилась передача данных с пакетной коммутацией, т.е. пакетный трафик отделяется от голосового))
- Передача коротких текстовых сообщений (SMS)
- Передача факсов
- Голосовая почта
- Конференцсвязь и мн. др.

Итак, рассмотрим основные элементы, входящие в состав системы GSM:

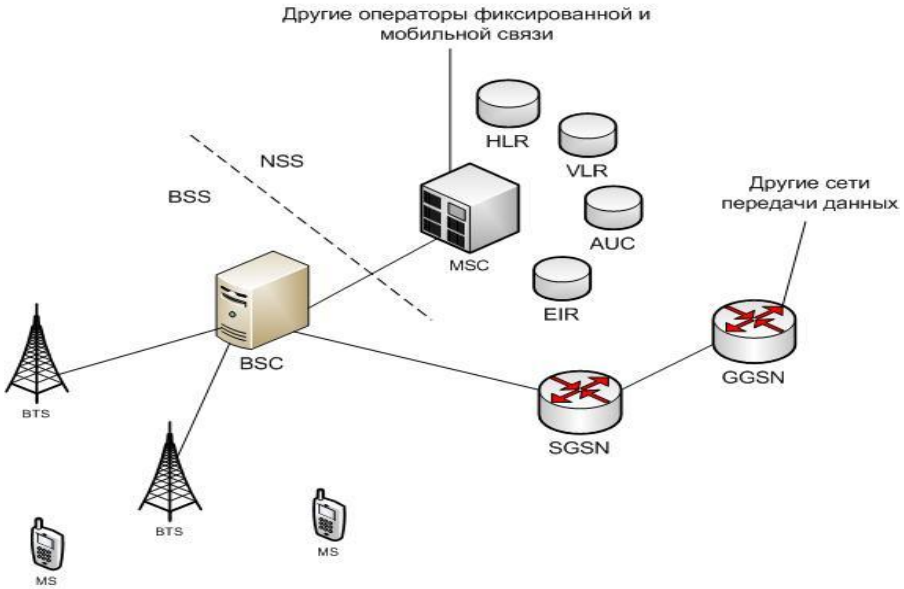


Рис. 7.118. Структура сети стандарта 2G (GSM)

Сеть GSM делится на 2 системы. Каждая из этих систем включает в себя ряд функциональных устройств, которые, в свою очередь являются компонентами сети мобильной радиосвязи.

Данными системами являются:

Система коммутации – Network Switching System (NSS).

Система базовых станций - Base Station System (BSS).

Система NSS выполняет функции обслуживания вызовов и установления соединений, а также отвечает за реализацию всех назначенных абоненту услуг. NSS включает в себя следующие функциональные устройства:

Центр коммутации мобильной связи (MSC).

Домашний регистр местоположения (HLR).

Визитный регистр местоположения (VLR).

Центр аутентификации (AUC).

Регистр идентификация абонентского оборудования (EIR).

Система BSS отвечает за все функции, относящиеся к радиоинтерфейсу. Эта система включает в себя следующие функциональные блоки:

Контроллер базовых станций (BSC).

Базовую станцию (BTS).

MS (т.е. телефон абонента (мобильная станция)) не принадлежит ни к одной из этих систем, но рассматривается как элемент сети.

Элементы сети, относящиеся к пакетной передачи данных:

SGSN – узел обслуживания абонентов.

GGSN – шлюзовой узел.

Стандарт 3G (UMTS)[2]

Разработка стандарта UMTS началась в 1992 году организацией по стандартизации IMT-2000. Впоследствии разработка этого стандарта была поручена 3GPP. Первая сеть UMTS была запущена в коммерческую эксплуатацию 1 декабря 2001 года в Норвегии. К маю 2010 года число абонентов переваливает за 540 миллионов по всему миру.

Скорость передачи данных для сетей UMTS может достигать 2Мбит/сек. Благодаря технологии HSDPA-High Speed Downlink Packet Access (3.5G), которая была внедрена в 2006 году максимальная скорость возросла до 14 Мбит/сек. Эти и другие преимущества UMTS позволяют предоставлять абонентам широкий перечень услуг: видеозвонки, видеоконференции, высококачественные голосовые звонки, загрузка файлов с высокой скоростью, сетевые игры, мобильная коммерция и мн. др.

Рассмотрим структуру системы UMTS и ее основные отличия от стандарта второго поколения GSM.

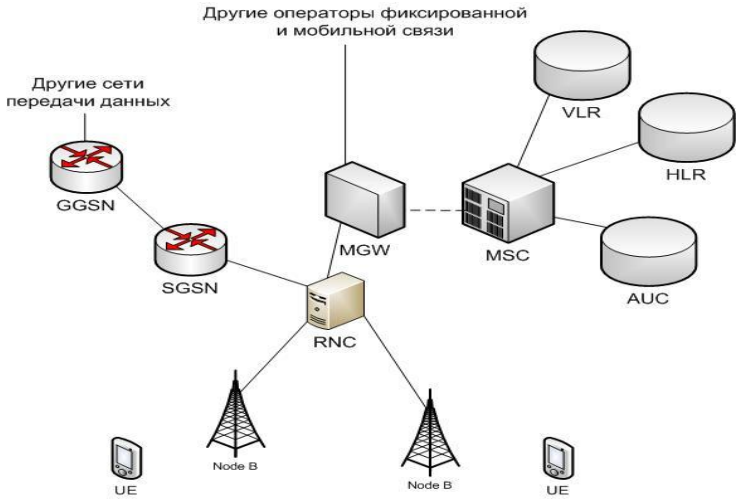


Рис. 7.119. Структура сети стандарта 3G (UMTS)

Подсистема коммутации

В первых релизах стандарта UMTS (R99, R4) подсистема коммутации не отличалась по своей структуре от той же подсистемы сетей второго поколения. В нее входили MSC – Mobile Switching Centre, который выполнял функции коммутации, установления соединения, тарификации и др., а также ряд регистров HLR, VLR, AUC, которые предназначены для хранения абонентских данных. В более поздних релизах (R5, R6, R7,R8) функции MSC были разделены между двумя устройствами: MSC-Server и MGW (Media gateway). MSC-Server отвечает за установление соединений, тарификацию, выполняет некоторые функции аутентификации. MGW представляет собой коммутационное поле, подчиненное MSC-Server.

Подсистема базовых станций:

В сети UMTS по сравнению с сетью GSM наибольшие изменения претерпела подсистема базовых станций. Отмеченные выше преимущества достигаются в первую очередь за счет новой технологии передачи информации между базовой станцией и телефоном абонента.

Итак, рассмотрим основные элементы, входящие в подсистему базовых станций:

RNC (Radio Network Controller) – контроллер сети радиодоступа системы UMTS. Он является центральным элементом подсистемы базовых станций и выполняет большую часть функций: контроль радиоресурсов, шифрование, установление соединений через подсистему базовых станций, распределение ресурсов между абонентами и др. В сети UMTS контроллер выполняет гораздо больше функций, нежели в системах сотовой связи второго поколения.

NodeB – базовая станция системы сотовой связи стандарта UMTS. Основной функцией NodeB является преобразование сигнала, полученного от RNC в широкополосный радиосигнал, передаваемый к телефону. Базовая станция не принимает решений о выделении

ресурсов, об изменении скорости к абоненту, а лишь служит мостом между контроллером и оборудованием абонента, и она полностью подчинена RNC.

Оборудование абонента получило название UE (User Equipment (мобильная станция)). Тем самым подчеркивается, что в отличие от предшествующих стандартов в UMTS может быть не только обычный телефон, но и смартфон, ноутбук, стационарный компьютер и т.п.

Пакетные данные в сети UMTS передаются от MGW к известному нам по системе GSM элементу SGSN (узел обслуживания абонентов), после чего через GGSN (шлюзовой узел) поступают к другим внешним сетям передачи данных, например Internet. Как правило, SGSN и GGSN сети GSM применяются для тех же целей и в сети UMTS. Производится только коррекция программного обеспечения данных элементов.

Стандарт LTE и его отличие от предыдущих стандартов

Стандарты третьего поколения позволяют предоставить широкий перечень мультимедийных услуг и поддерживают скорости передачи данных до 14Мбит/сек. Это вполне соответствует запросам абонентов в настоящее время. Однако, объемы передаваемой информации в телекоммуникационных сетях растут с каждым днем. Чтобы удовлетворить потребности пользователей по скорости передачи данных и набору услуг, хотя бы на 20 лет вперед необходим новый стандарт, уже четвертого поколения.

Работа над первым стандартом четвертого поколения - LTE (Long Term Evolution) началась в 2004 году организацией 3GPP. Главными требованиями, которые предъявлялись в процессе работы над стандартом были следующие:

- Скорость передачи данных выше 100 Мбит/сек.
- Высокий уровень безопасности системы.
- Высокая энергоэффективность.
- Низкие задержки в работе системы.
- Совместимость со стандартами второго и третьего поколений.

В конце 2009 года в Швеции была запущена в коммерческую эксплуатацию первая сеть стандарта LTE.

Сети LTE поддерживают скорости передачи данных до 326,4 Мбит/сек. К примеру, загрузка фильма в хорошем качестве займет менее одной минуты. Таким образом, верхняя планка по скорости передачи данных практически снимается.

Рассмотрим структуру сети LTE:

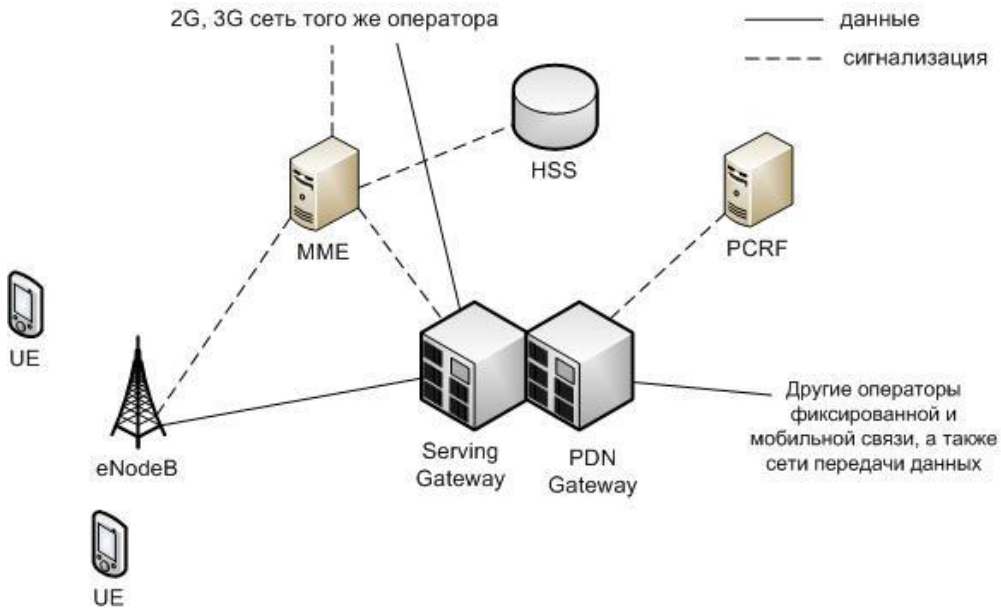


Рис. 7.120. Структура сети стандарта LTE

Из схемы сети LTE, представленной выше, уже видно, что структура сети сильно отличается от сетей стандартов 2G и 3G. Существенные изменения претерпела и подсистема базовых станций, и подсистема коммутации. Была изменена технология передачи данных между оборудованием пользователя и базовой станцией. Также подверглись изменению и протоколы передачи данных между сетевыми элементами. Вся информация (голос, данные) передается в виде пакетов. Таким образом, уже нет разделения на части обрабатывающие либо только голосовую информацию, либо только пакетные данные.

Можно выделить следующие основные элементы сети стандарта LTE:

Serving SAE Gateway или просто Serving Gateway (SGW) – обслуживающий шлюз сети LTE. Предназначен для обработки и маршрутизации пакетных данных поступающих из/в подсистему базовых станций. По сути, заменяет MSC (выполняет функции коммутации, установления соединения, тарификации), MGW (представляет собой коммутационное поле) и SGSN (узел обслуживания абонентов пакетной сети передачи данных) сети UMTS (3G). SGW имеет прямое соединение с сетями второго и третьего поколений того же оператора, что упрощает передачу соединения в/из них по причинам ухудшения зоны покрытия, перегрузок и т.п.

Public Data Network (PDN) SAE Gateway или просто PDN Gateway (PGW) – шлюз к/от сетей других операторов. Если информация (голос, данные) передаются из/в сети данного оператора, то они маршрутизируются именно через PGW.

Mobility Management Entity (MME) – узел управления мобильностью. Предназначен для управления мобильностью абонетов сети LTE.

Home Subscriber Server (HSS) – сервер абонентских данных. HSS представляет собой объединение VLR (гостевой регистр местоположения), HLR (домашний регистр

местоположения), AUC (центр аутентификации абонентов) выполненных в одном устройстве.

Policy and Charging Rules Function (PCRF) – узел выставления счетов абонентам за оказанные услуги связи.

Все перечисленные выше элементы относятся к системе коммутации сети LTE. В системе базовых станций остался лишь один знакомый нам элемент – базовая станция, которая получила название eNodeB. Этот элемент выполняет функции и базовой станции, и контроллера базовых станций сети LTE. За счет этого упрощается расширение сети, т.к. не требуется расширение емкости контроллеров или добавления новых. Мобильная станция представлена – UE.

Интерфейсы между узловыми элементами в сетях стандарта LTE

Структура сети стандарта LTE претерпела значительные изменения по сравнению с сетями предыдущих поколений. Это повлияло также и на изменение интерфейсов между узлами сети. На рисунке ниже представлена общая модель сети стандарта LTE и ее основные интерфейсы.

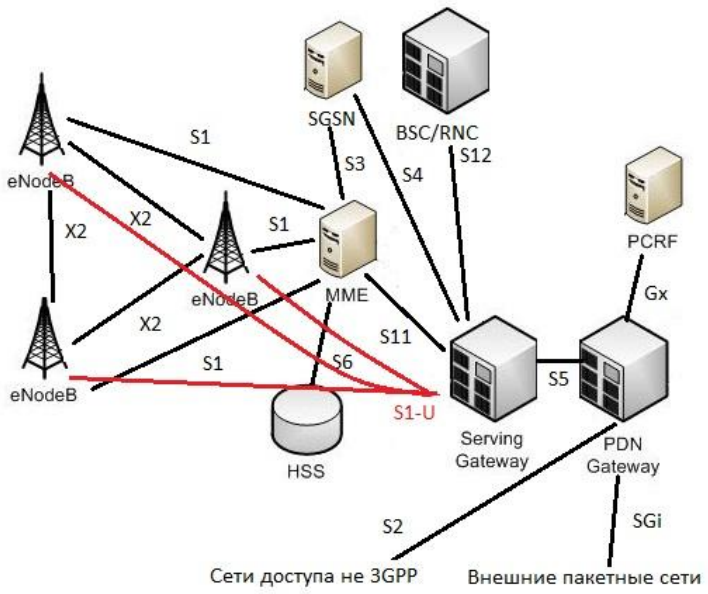


Рис. 7.121. Интерфейсы сети стандарта LTE

Рассмотрим основные интерфейсы сети LTE:

X2 - интерфейс между eNodeB. Базовые станции в сети LTE соединены по принципу «каждый с каждым».

S1 – интерфейс связывающий подсистему базовых станций E-UTRAN и MME. По данному интерфейсу передаются данные управления.

S1-U – интерфейс между E-UTRAN и SAE, по которому передаются пользовательские данные.

S2 – интерфейс для организации соединения между PDN-Gateway и сетями доступа, которые не разрабатывались 3GPP.

S3 – интерфейс, предоставляющий прямое соединение SGSN и MME. Он служит для передачи данных управления для обеспечения мобильности между LTE и 2G/3G сетями.

S4 – интерфейс, связывающий SAE и SGSN. Он служит для передачи пользовательских данных для обеспечения мобильности между LTE и 2G/3G сетями.

S5 – интерфейс между SAE и PDN-Gateway. S5 предназначен для передачи пользовательских данных между SAE и PDN-Gateway.

S6 – интерфейс между MME и HSS. Он используется для передачи данных абонентского профиля, а также осуществления процедур аутентификации в сети LTE.

Gx – интерфейс между PDN-Gateway и PCRF. Gx предназначен для передачи правил тарификации от PCRF к PDN-Gateway.

SGi - интерфейс между PDN-Gateway и внешними IP-сетями.

Принципы построения радиоинтерфейса LTE в Downlink (от БС к МС)

Одной из главных отличительных особенностей стандарта LTE, которая позволяет достигать высоких скоростей передачи данных является изменение принципов построения интерфейса от eNodeB (БС) до UE (МС) на линии «вниз». Рассмотрим главные особенности этого интерфейса и постараемся выделить основные качественные отличия, которые отличают этот стандарт от других.

В сетях связи стандарта LTE в Downlink (DL) используется модуляция OFDM – Orthogonal Frequency Devision Multiplexing– ортогональная частотная модуляция. Этот тип модуляции определяет и принцип доступа OFDMA - Orthogonal Frequency Devision Multiple Access – множественный доступ с ортогональным частотным разделением каналов. Суть его заключается в том, что все частотно-временное поле, выделенное для работы оператора, разделяется на небольшие блоки. Причем они небольшие как по частоте (15 кГц), так и по времени (0,5 мс). Сеть распределяет эти блоки между абонентами в зависимости от их потребностей и возможностей сети. Таким образом, обеспечивается максимально эффективное использование ресурсов.

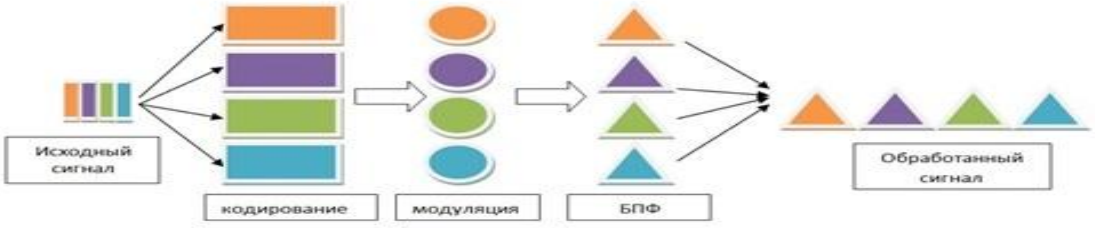


Рис. 7.122. OFDM – модулятор

Ниже перечислены главные шаги преобразования сигнала в OFDM модуляторе.

1) Разделение исходного потока бит на параллельные потоки.

2) Кодирование помехоустойчивым кодом, в процессе которого значительно увеличивается число символов в отдельных потоках.

3) Манипуляция выбранным в данный конкретный момент способом модуляции: QPSK, 16QAM, 64QAM.

4) Перемножение полученной последовательности каждого потока на свою поднесущую. Эта операция является ключевой и будет рассмотрена ниже.

5) Объединение сигналов и передача в эфир.

Умножение сигнала на свою поднесущую перемещает сигнал в нужное частотное пространство. Также на этом этапе происходит преобразование сигнала из временной области в частотную. Это выполняется благодаря БПФ – быстрому преобразованию Фурье. Эти две процедуры позволяют добиться максимально близкого размещения сигналов в частотной области и сократить до минимума защитные интервалы. Это достигается благодаря тому, что поднесущие выбираются ортогональными (на практике квазиортогональными), и отдельные потоки относительно легко выделить на приемной стороне.

Кроме использования OFDMA в LTE – есть еще одно важное новшество: обязательное (в отличие от UMTS) использование MIMO - Multiple Input Multiple Output – множественный вход множественный выход. При этом информационный поток направляется между сторонами обмена информации несколькими «путями», что обеспечивает более эффективное использование частотно-временного ресурса.

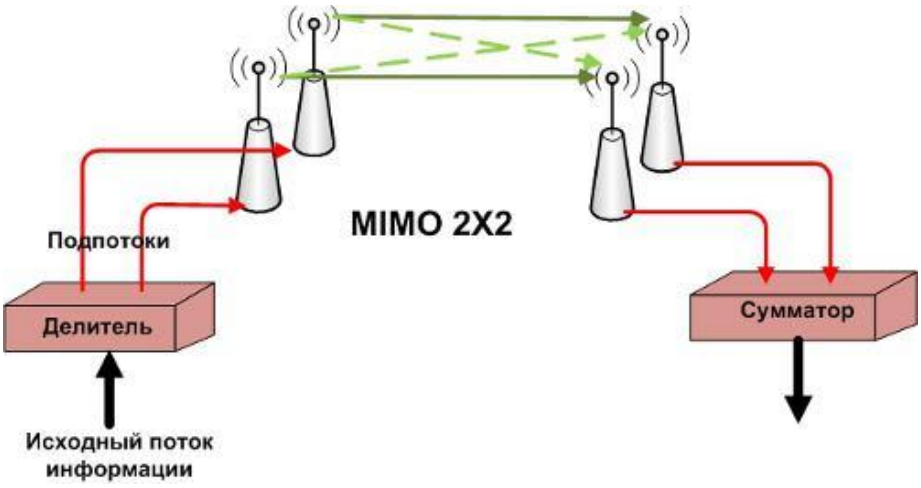


Рис. 7.123. MIMO 2x2

Эти два важных изменения позволяют добиться скорости передачи данных в Downlink свыше 100 Мбит/сек. Задержки передачи данных не превышают 20 мс. Для сравнения в

UMTS скорости передачи данных редко поднимаются свыше 20 Мбит/сек, а задержки могут колебаться от 40 до 100 мс.

Принципы построения радиоинтерфейса LTE в Uplink (от МС к БС)

В сетях связи стандарта LTE скорость передачи данных в направлении от UE (МС) к eNodeB (БС) может достигать 50 Мбит/сек, а задержки не превышают 10мс. Эти показатели на много превышают значения в сетях третьего поколения и практически сравнялись с проводными выделенными каналами связи. Рассмотрим главные особенности построения радиоинтерфейса Uplink в стандарте LTE.

В отличие от радиоинтерфейса Downlink, где информация одного пользователя может передаваться на разных поднесущих, в Uplink данные каждого пользователя передаются в одной полосе частот, причем в одно и то же время. Однако это не означает, что информационные потоки накладываются друг на друга и необратимо искажаются. Это обеспечивается благодаря использованию множественного доступа с частотным разделением с единственной несущей частотой SC-FDMA (Single Carrier Frequency Devision Multiple Access). Рассмотрим основные принципы работы SC-FDMA – модулятора.

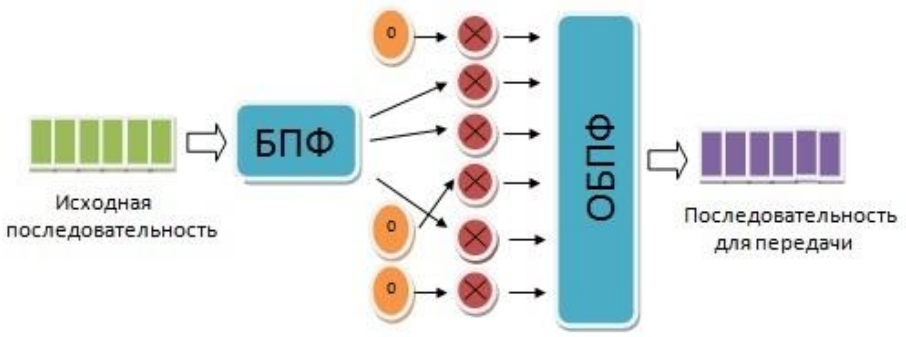


Рис. 7.123 - SC-FDMA – модулятор

Первым этапом исходная информационная последовательность, предназначенная для передачи от абонента, преобразуется в частное представление с помощью быстрого преобразования Фурье (БПФ). Далее, в зависимости от скорости потока от данного абонента, сеть выделяет UE (МС) несколько поднесущих, среди которых распределяются преобразованный поток. Те поднесущие, которые используют другие пользователи не занимаются в данном абонентском терминале, а соответствующие поднесущие перемножаются с «0». После обратного быстрого преобразования Фурье (ОБПФ) модулированные потоки объединяются и переводятся обратно во временную область. Не смотря на то, что данные передаются от разных устройств в сети в одно и то же время в одной и той же полосе частот, на приемной стороне после обратных сказанным выше процедур, можно выделить информационные потоки от отдельных UE (МС).

Благодаря использованию SC-FDMA в системе LTE удалось достигнуть трехкратного увеличения спектральной эффективности на линии «вверх», по сравнению с сетями 3G.

Логические каналы на радиоинтерфейсе в LTE

Одной из важнейших составляющих радиоинтерфейса любой подвижной системы связи, которая обеспечивает заданные характеристики ее работы, является структура логических, транспортных и физических каналов. Рассмотрим логические параметры сети связи LTE.

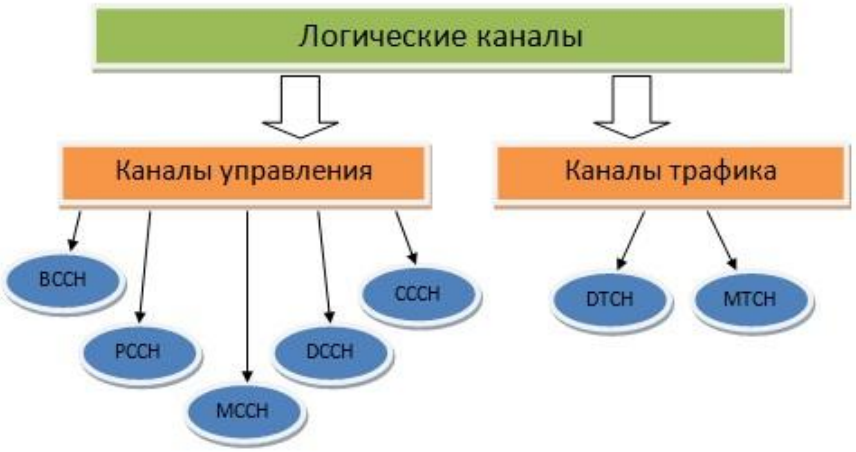


Рис. 7.124. Логические каналы LTE

Логические каналы подразделяются по типам передаваемой информации на каналы управления и на трафиковые каналы.

К каналам управления относятся:

 BCCH (Broadcast Control Channel) – вещательный канал управления – служит для передачи системной служебной информации в Downlink.

 PCCH (Paging Control Channel) – пейджинговый канал управления – предназначен для передачи пейджинговых сообщений к UE (МС) от eNodeB (БС).

 MCCH (Multicast Control Channel) – многопользовательский канал управления – необходим для передачи служебной информации одновременно к нескольким абонентским устройствам.

 DCCH (Dedicated Control Channel) – выделенный канал управления – служит для передачи служебной информации между конкретным абонентским устройством и сетью.

 CCCH (Common Control Channel) – общий канал управления – предназначен для обмена служебной информацией между UE (МС) и сетью в процедурах начального доступа UE (МС) в сеть до организации выделенного канала.

К трафиковым каналам относятся:

 DTCH (Dedicated Traffic Channel) – выделенный трафиковый канал – основной канал для передачи пользовательских данных между одним конкретным UE (МС) и сетью.

 MTCH (Multicast Traffic Channel) – многопользовательский трафиковый канал – служит для передачи широковещательной трафиковой информации. Хорошим примером использования этого канала может служить трансляция радио или ТВ-программ.

Транспортные каналы на радиоинтерфейсе в LTE

На радиоинтерфейсе в сети стандарта LTE применяется стек каналов для передачи данных между абонентским терминалом и сетью. Низший уровень в этом стеке образуют физические каналы. По ним передаются транспортные, которые в свою очередь несут логические каналы.

Рис. 7.125. Транспортные каналы LTE

Рассмотрим виды транспортных каналов на радиоинтерфйсе сети стандарта LTE. Все транспортные каналы можно классифицировать по направлению передачи: Uplink (от UE (МС) к eNodeB (БС)) и Downlink (от eNodeB (БС) к UE (МС)).

К транспортным каналам в Downlink относятся:

 BCH (Broadcast Channel) – широковещательный канал.

 PCH (Paging Channel) – канал для пейджинга.

 DL-SCH (Downlink Shared Channel) – общий канал для передачи данных вниз.

 MCH (Multicast Channel) – многопользовательский канал.

К транспортным каналам в Uplink относятся:

 RACH (Random Access Channel) – канал случайного доступа.

 UL-SCH (Downlink Shared Channel) – общий канал для передачи данных вверх.

Как было сказано выше, транспортные каналы передаются в логических каналах. На рисунке ниже представлена связь между логическими и транспортными каналами в LTE.

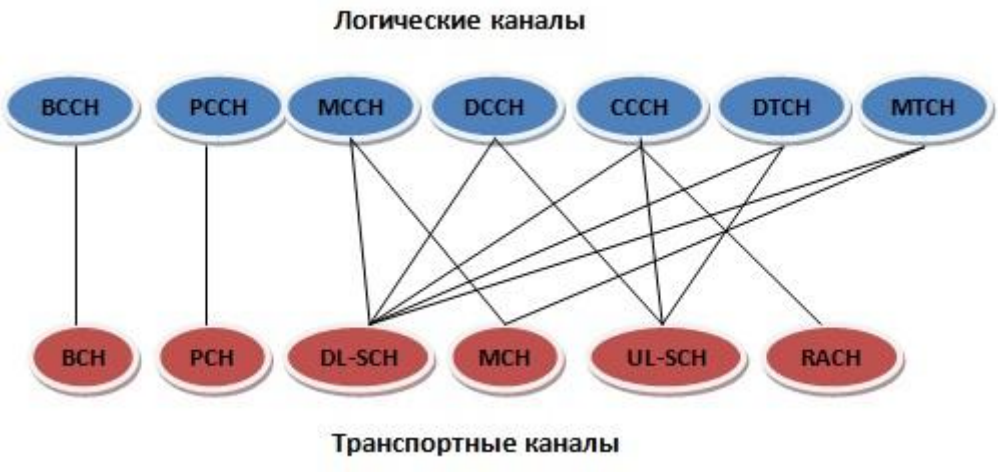


Рис. 7.126. Связь логических и транспортных каналов

Физические каналы на радиоинтерфейсе в LTE

Информация между UE (МС) и eNodeB (БС) передается не произвольным образом, а через четко организованную структуру каналов. Рассмотрим классификацию, виды и назначение физических каналов в сети LTE.

Рис. 7.127. Физические каналы LTE

Физические каналы можно классифицировать по направлению передачи информации: Downlink и Uplink.

К физическим каналам в Downlink относятся:

PDSCH (Physical Downlink Shared Channel) - физический распределенный канал в направлении «вниз» - служит для высокоскоростной передачи мультимедийной информации.

PDCCH (Physical Downlink Control Channel) – физический канал управления в направлении «вниз» - предназначен для передачи информации для управления конкретным UE (МС).

CCPCH (Common Control Physical Channel) – общий физический канал управления – необходим для передачи общей для всех информации.

К физическим каналам в Uplink относятся:

PRACH (Physical Random Access Channel) – физический канала произвольного доступа – служит для первичного доступа в сеть.

PUCCH (Physical Uplink Control Channel) – физический канал управления в направлении «вверх» - необходим для передачи служебной информации от конкретной UE (МС) к eNodeB (БС).

PUSCH (Physical Uplink Shared Channel) – физический распределенный канал в направлении «вверх» - предназначен для высокоскоростной передачи данных в Uplink.

Связь между транспортными и физическими каналами представлена на рисунке ниже.

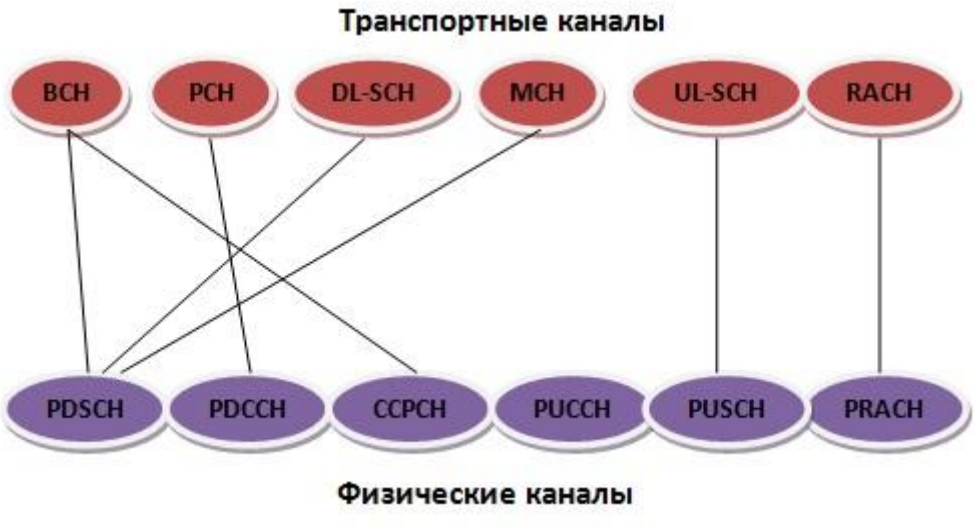


Рис. 7.128. Связь физических и транспортных каналов

Основные параметры LTE

Таблица 7.17. Основные параметры LTE

Название параметра	Параметр
Uplink (UL): восходящее соединение	SC-FDMA
Downlink (DL): нисходящее соединение	OFDMA
Ширина частотного диапазона, МГц	1,4; 3, 5; 10; 15; 20
Минимальный интервал между кадрами, мс	1
Шаг (частотный интервал) между поднесущими, кГц	15

Стандартная длина префикса CP, мкс	4,7
Увеличенная длина префикса CP, мкс	16,7
Схемы модуляции (Uplink)	BPSK, QPSK, 8PSK, 16QAM
Схемы модуляции (Downlink)	QPSK, 16QAM, 64QAM
Пространственное мультиплексирование	Один канал для Uplink-трафика на каждый абонентский терминал; До 4 каналов для Downlink-трафика на каждый абонентский терминал; MU-MIMO с поддержкой для восходящего (Uplink) и нисходящего (Downlink) соединений

Практическая реализация

Как было сказано выше, на практике будет реализован канал Downlink системы мобильной связи стандарта LTE. Структура данного канала представлена на рисунке 7.129

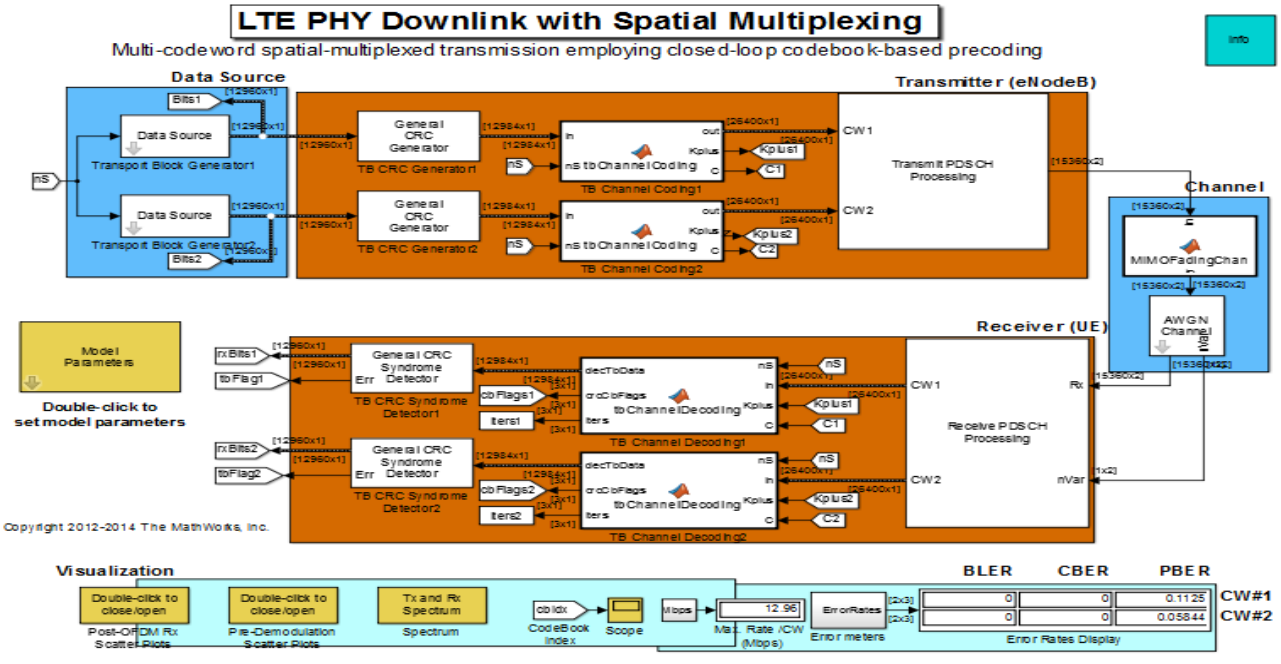


Рис. 7.129. Канал Downlink LTE Simulink MATLAB 2015b

Рассмотрим более подробно данный канал.

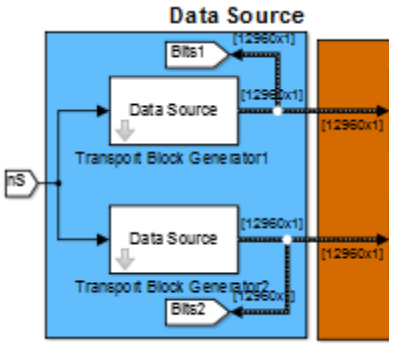


Рис. 7.130. Разделение исходного потока бит на параллельные потоки

Кодирование помехоустойчивым кодом, в процессе которого значительно увеличивается число символов в отдельных потоках. В данной схеме используется код CRC.

Каждый отдельный параллельный поток кодируется данным кодом с заданным полиномом.

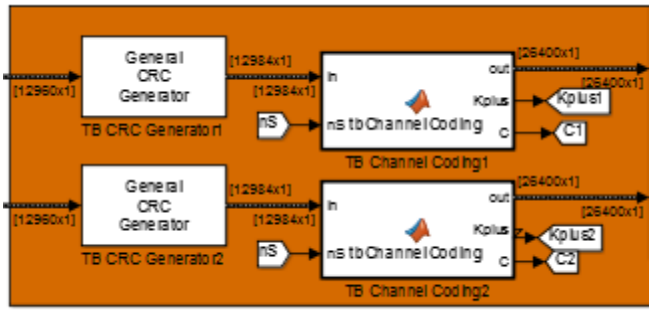


Рис. 7.131. Кодирование помехоустойчивым кодом

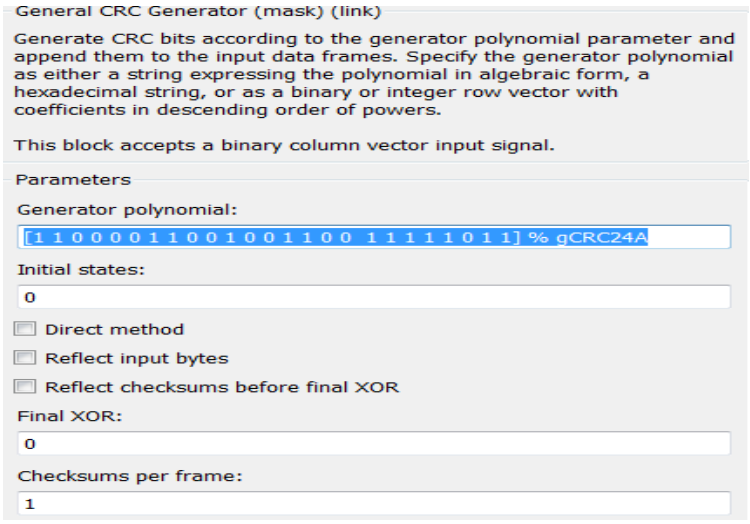


Рис. 7.132. Параметры CRC кодера

Манипуляция выбранным в данный конкретный момент способом модуляции. В канале Downlink используются методы манипуляции: QPSK, 16QAM, 64QAM. Далее перемножение

полученной последовательности каждого потока на свою поднесущую и БПФ (так называемая OFDM – модуляция). Где в результате получаем один сложный сигнал.

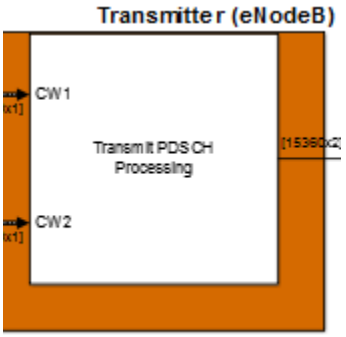


Рис. 7.133. Манипуляция выбранным в данный конкретный момент способом модуляции

Структура этого блока имеет следующий вид:

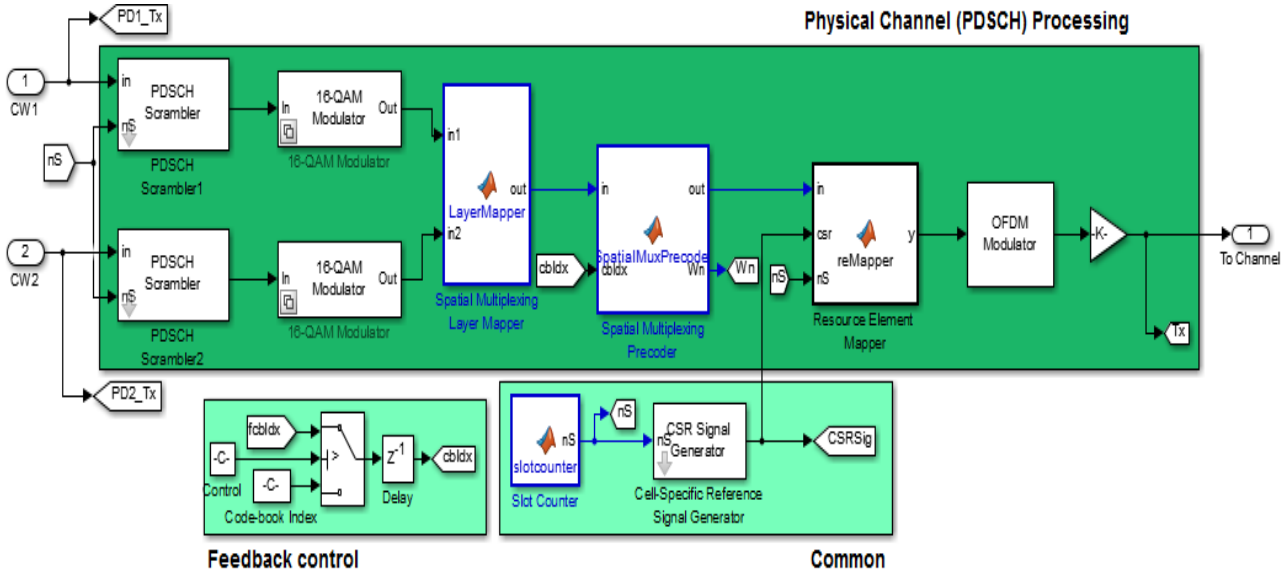


Рис. 7.134. Квадратурная манипуляция и получение OFDM символов

Передача в эфир. Для этого используется технология MIMO 2x2 или 4x4 приемных/передающих антенн. Где один общий поток (сигнал) разделяется на 2 потока (2x2 антенна) или 4 потока (4x4 антенна).

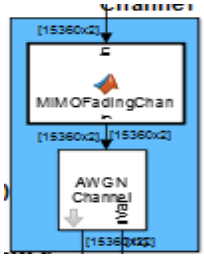


Рис. 7.135. Передача в эфир

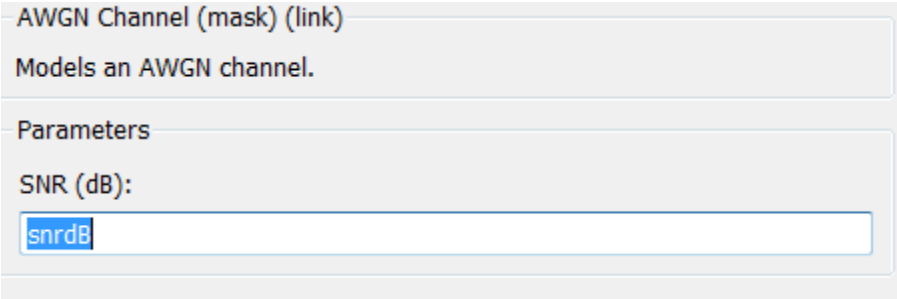


Рис. 7.136. Характеристики блока БГШ (AWGN)

Далее подпотоки MIMO объединяются в один поток, который приходит на мобильную станцию под воздействием помех.

Далее мобильная станция производит обратные преобразования, реализованные выше, а именно, получаем паралельные потоки. Потом производится обратное быстрое преобразование Фурье (ОБПФ). Затем производится демодуляция.

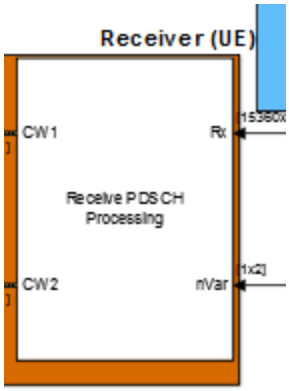


Рис. 7.137. Паралельные потоки-ОБПФ-демодуляция

Схема, входящая в данный блок:

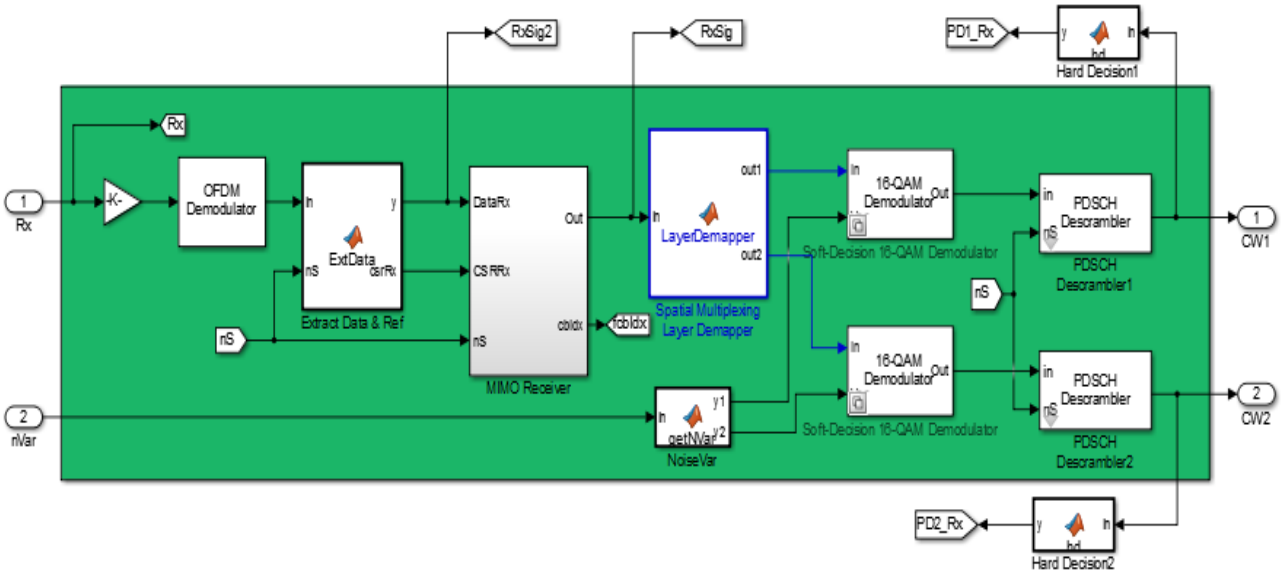


Рис. 7.138. Паралельные потоки-ОДПФ-демодуляция

Далее производится декодирование по соответствующему алгоритму CRC:

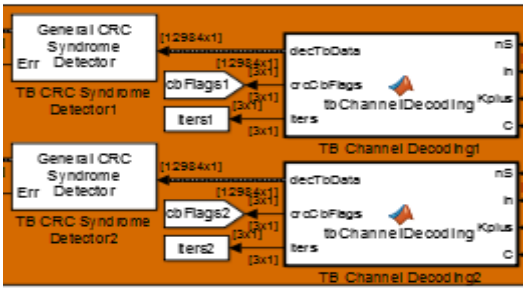


Рис. 7.139. Декодирование CRC

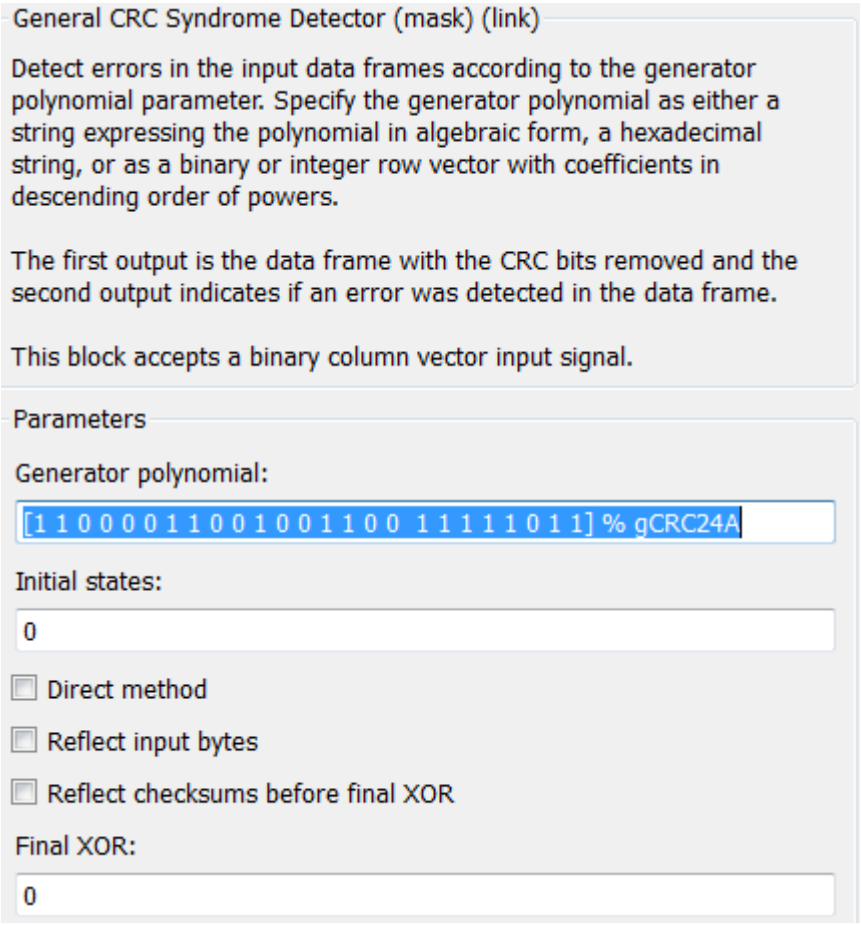


Рис. 7.140. Характеристики декодера CRC

После декодирования производится преобразование параллельных потоков в один исходный поток:

Рис. 7.141. Получение исходного потока

Данная схема позволяет формировать характеристики передачи данных по этому каналу, а именно это ширина спектра, количество антенн в MIMO, вид модуляции, отношение сигнал/шум:

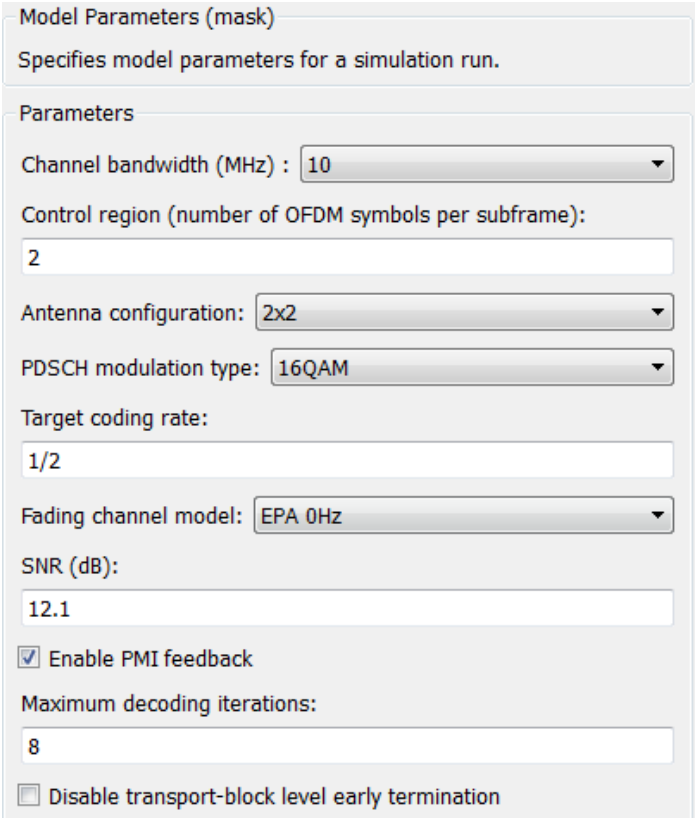


Рис. 7.142. Характеристики канала

В результате работы схемы можно получить некоторые зависимости:

Спектр передаваемого и принятого сигнала.

Диаграмму созвездий передаваемого и принятого сигнала (для каждой из антенн MIMO).

Итерации декодера в зависимости от времени и кодовых слов для каждого параллельного потока.

Также можно построить зависимость битовой вероятности ошибки при заданном отношении сигнал/шум каждого параллельного потока отдельно, меняя значения отношения сигнал/шум.

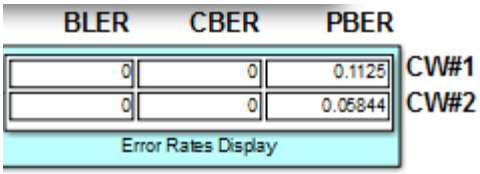


Рис. 7.143. Информация о битовой вероятности ошибки параллельных потоков

В качестве примера зададим следующие характеристики передачи данных:

Ширина спектра - 10 МГц.

Количество антенн MIMO – 4x4.

Модуляция – QPSK.

Отношение сигнал/шум – 1 дБ.

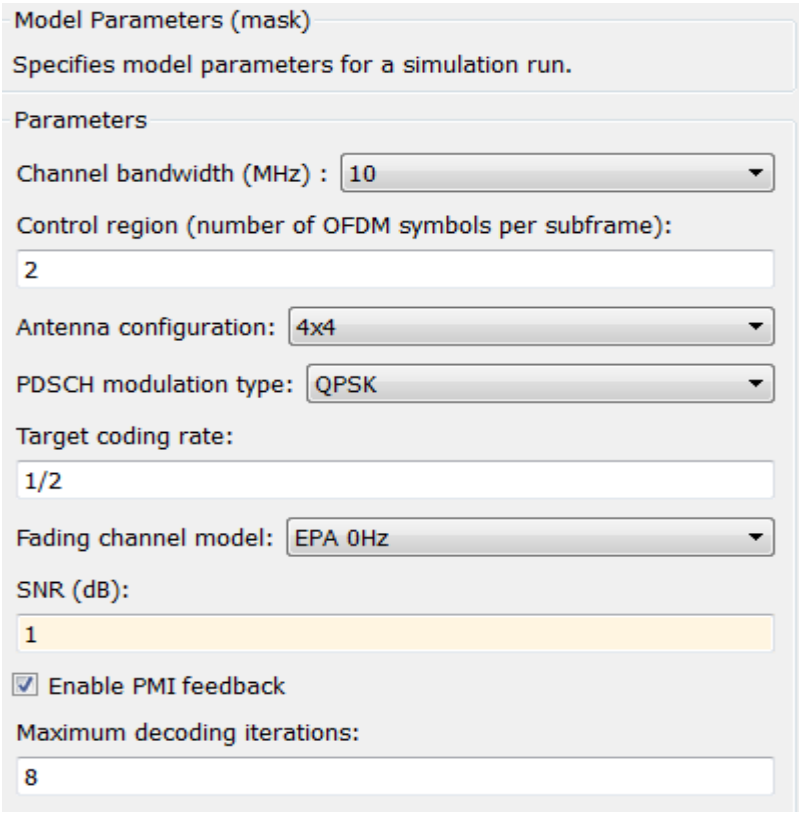


Рис. 7.144. Характеристики передачи данных

В результате получим следующие зависимости:

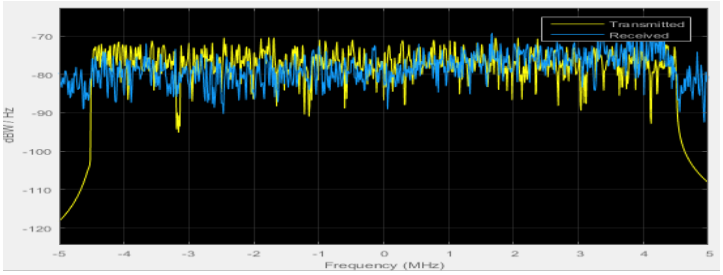


Рис. 7.145. Спектр входного (желтым) и выходного (синим) сигналов

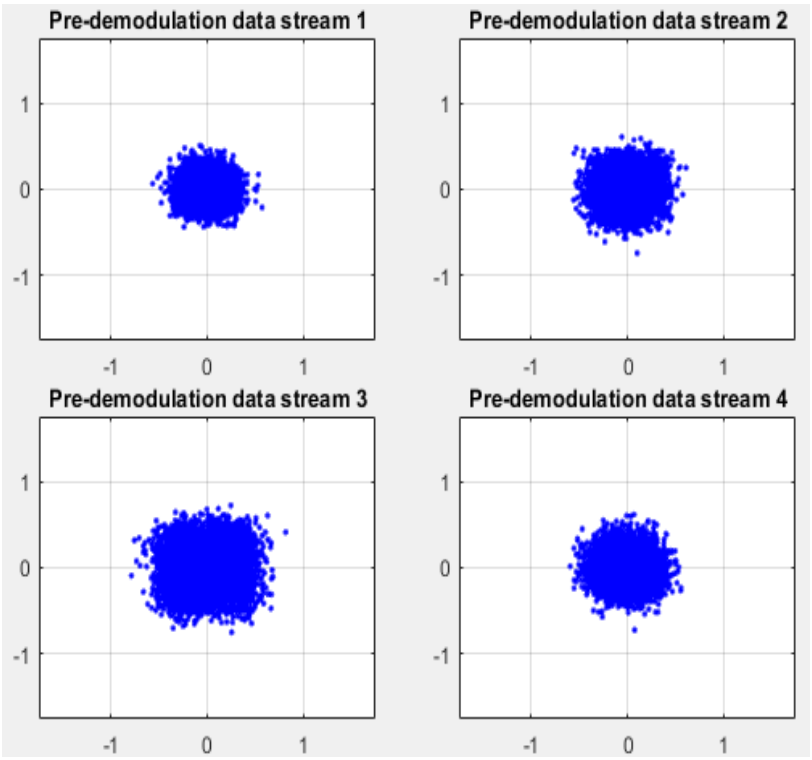


Рис. 7.146. Диаграмма созвездий переданного сигнала для каждой из антенн MIMO

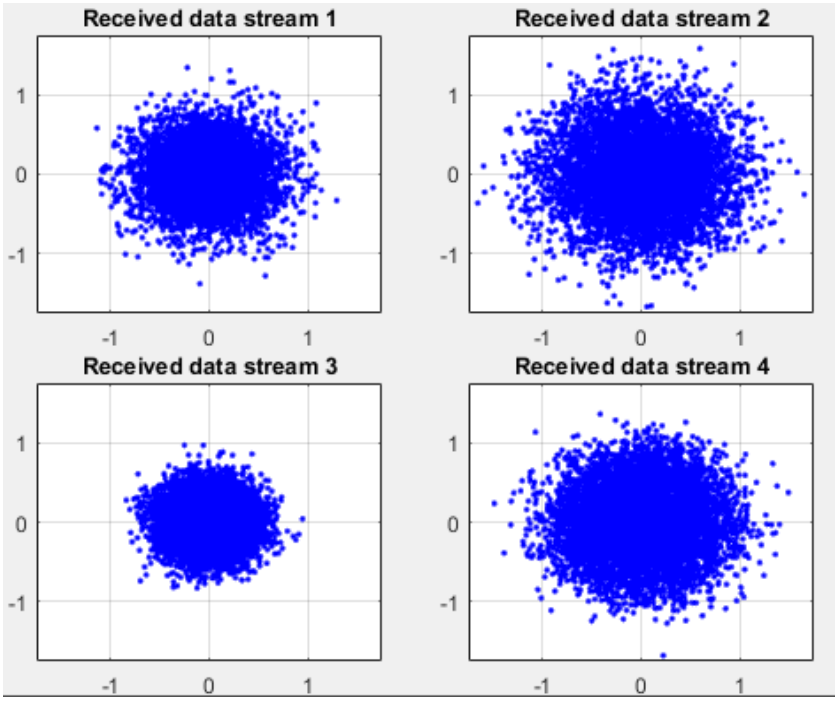


Рис. 7.147. Диаграмма созвездий принятого сигнала для каждой из антенн MIMO

На основании полученных значений, построим зависимость.

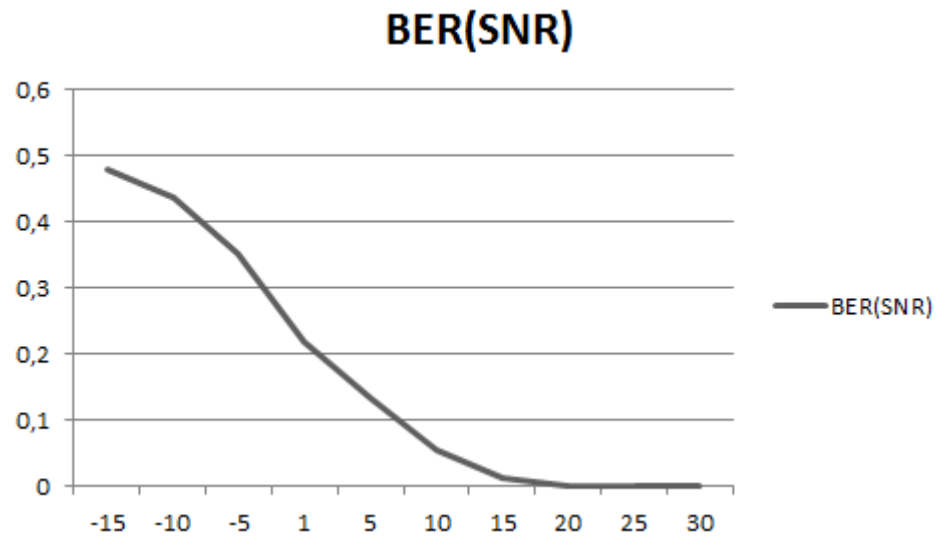


Рис. 7.148. Зависимость битовой вероятности ошибки от отношения сигнал/шум для первого потока

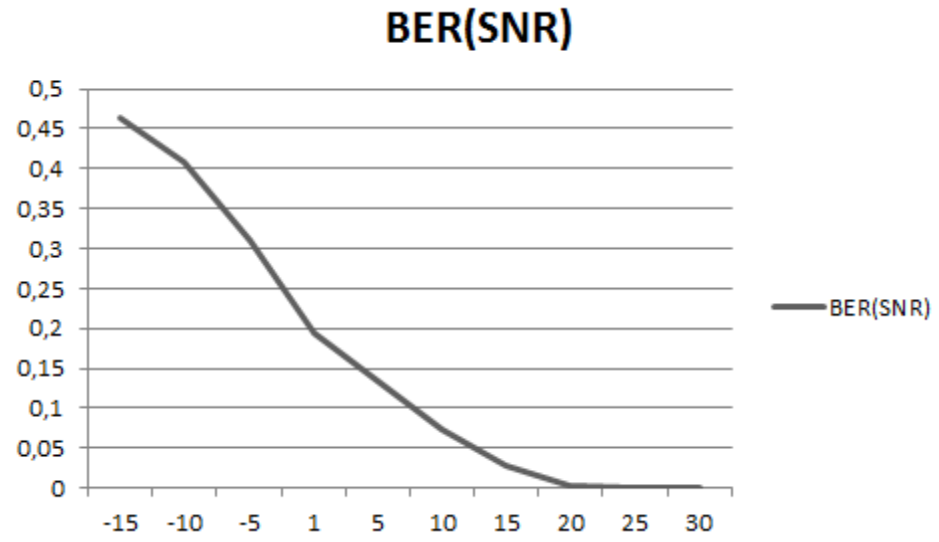


Рис. 7.149. Зависимость битовой вероятности ошибки от отношения сигнал/шум для второго потока

В качестве еще одного примера зададим следующие характеристики передачи данных:

Ширина спектра - 10 МГц.

Количество антенн MIMO – 2x2.

Модуляция – QPSK.

Отношение сигнал/шум – 1 дБ.

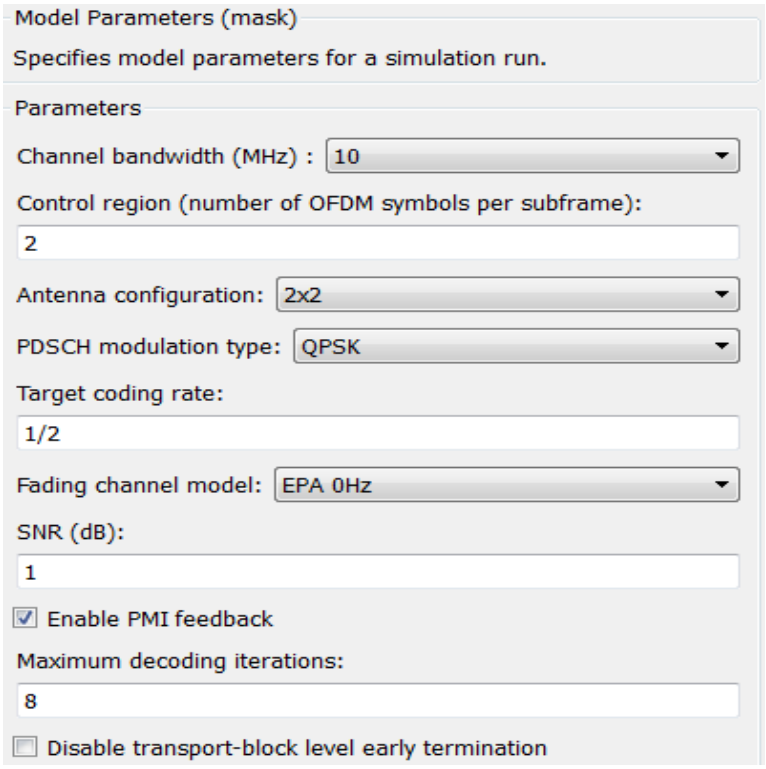


Рис. 7.150. Характеристики передачи данных

В результате получим следующие зависимости:

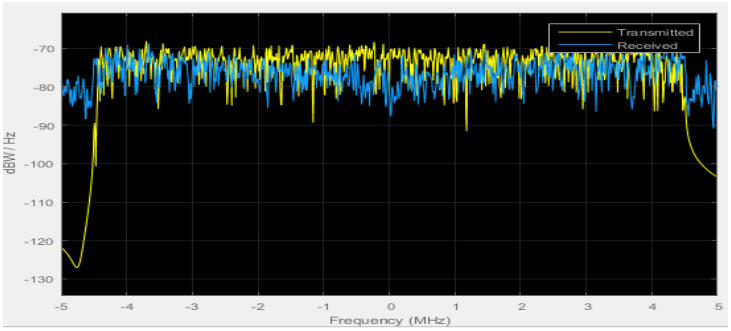


Рис. 7.151. Спектр входного (желтым) и выходного (синим) сигналов

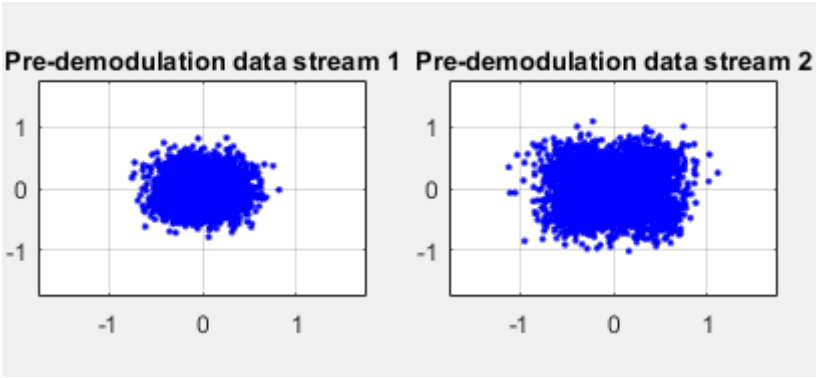


Рис. 7.152. Диаграмма созвездий переданного сигнала для каждой из антенн MIMO

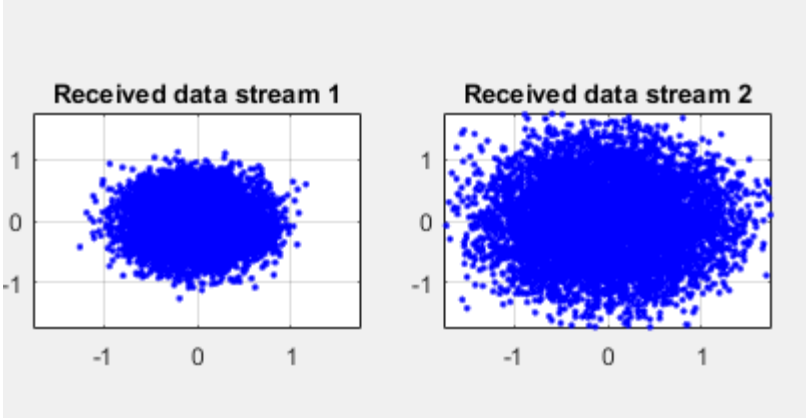


Рис. 7.153. Диаграмма созвездий принятого сигнала для каждой из антенн MIMO

Изменим отношение сигнал/шум – -15, -10, -5, 1, 5, 10, 15, 20, 25 и 30 дБ и построим зависимость битовой вероятности ошибки от отношения сигнал/шум для десяти точек для обоих параллельных потоков

На основании полученных значений, построим зависимость.

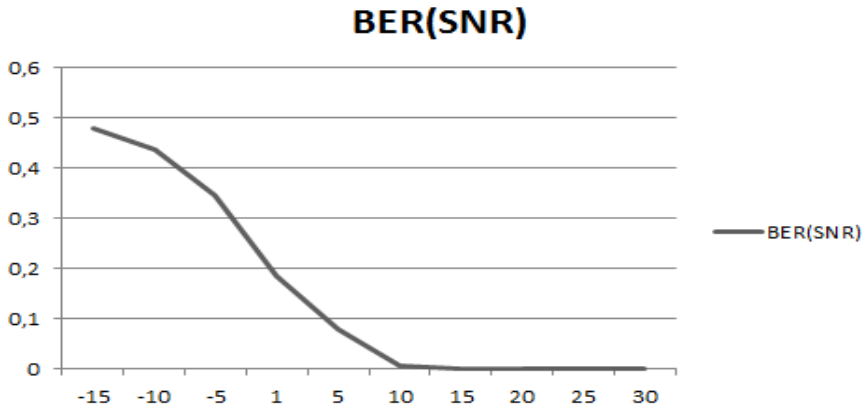


Рис. 7.154. Зависимость битовой вероятности ошибки от отношения сигнал/шум для первого потока

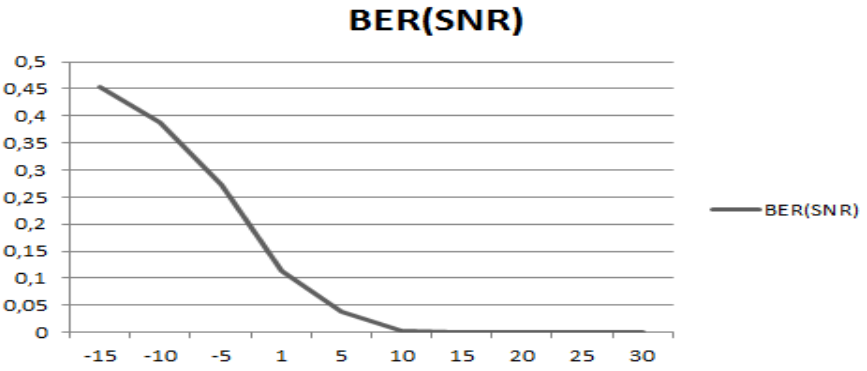


Рис. 7.155. Зависимость битовой вероятности ошибки от отношения сигнал/шум для второго потока

Методика и проведение исследования канала Downlink

Запустить Matlab 15 от имени администратора (обязательно).

В результате запуска на экране монитора появится следующее окно:

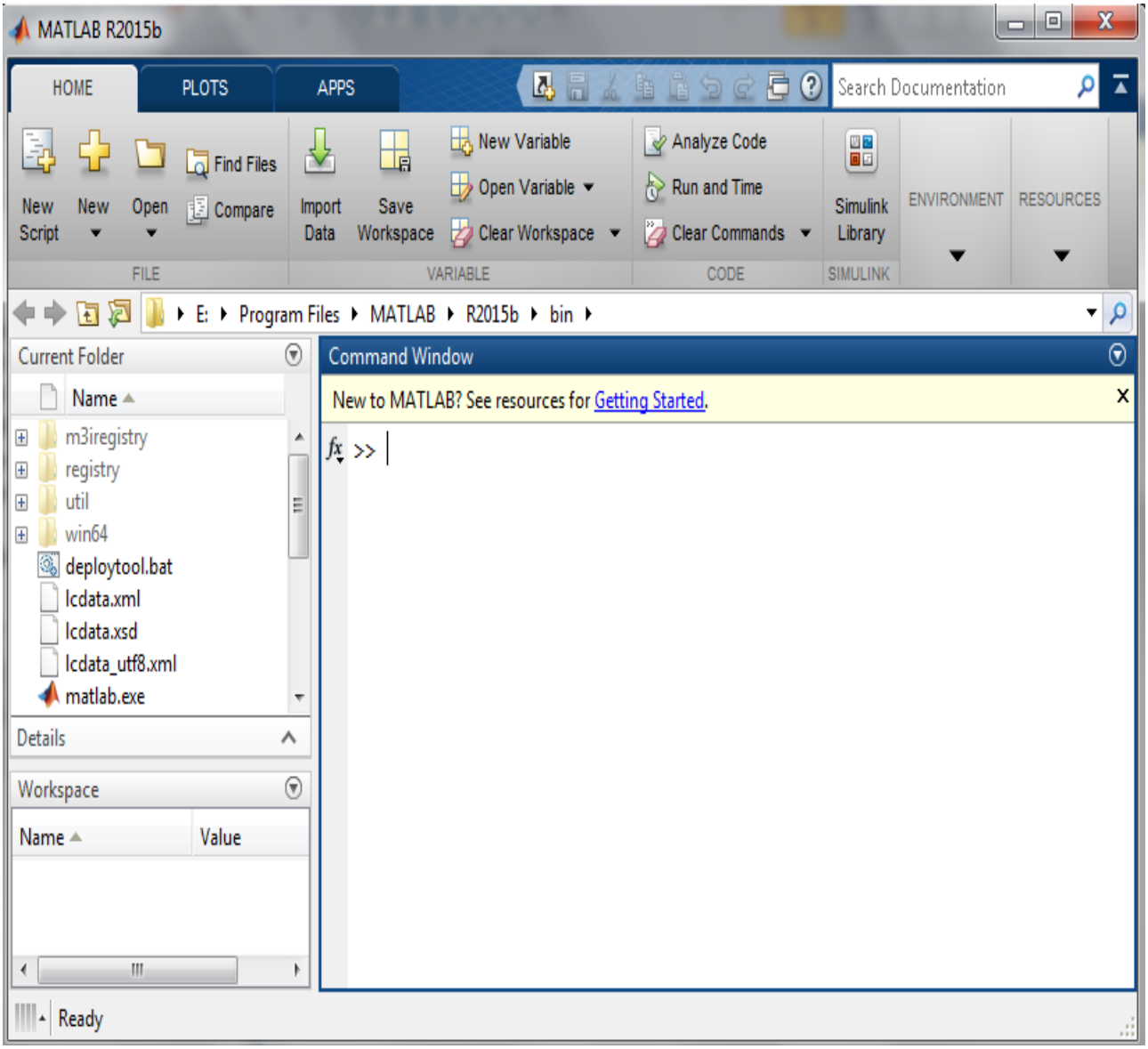


Рис. 7.156. Диалоговое окно Matlab 15

В командной строке программы прописать: cd ../ (при пропуске данного пункта могут возникнуть проблемы при компиляции).

В командной строке программы прописать LTEDownlinkExample, в результате откроется окно со схемой в программе, которое имеет следующий вид:

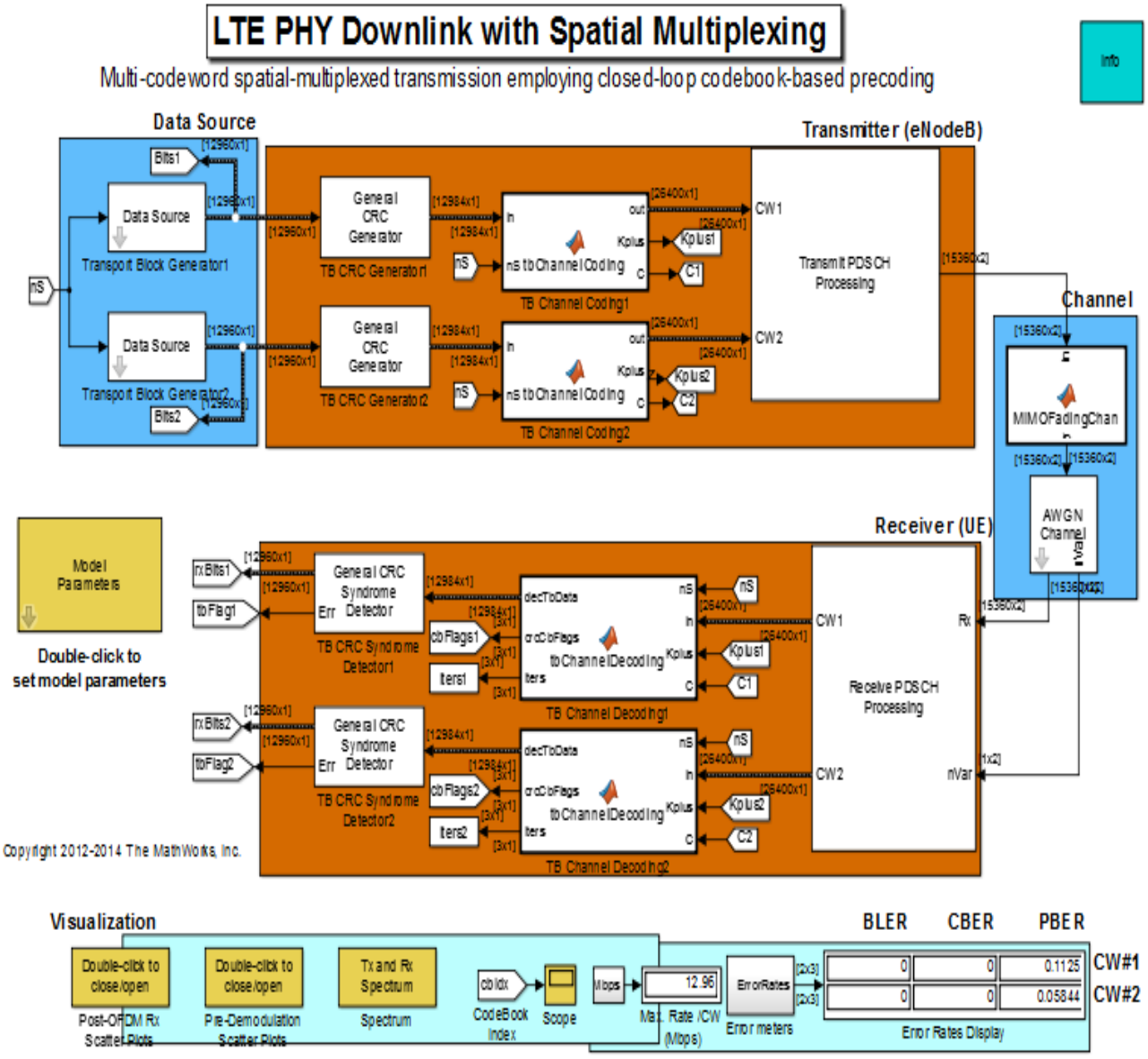


Рис. 7.157. Схема канала Downlink

Задать следующие характеристики передачи данных:

Модуляция – QAM-16.

Количество антенн MIMO 2x2.

Ширина спектра – 10 МГц.

Изменять отношение сигнал/шум – -15, -10, -5, 1, 5, 10, 15, 20, 25, 30 дБ (SNR) и на каждом его значении фиксировать в отчете выходные зависимости, а именно спектр переданного и принятого сигналов, диаграммы созвездий на каждой из антенн MIMO для переданного и принятого сигналов, итерации декодера в зависимости от времени и кодовых слов первого потока и второго потока. Так же на каждом шаге фиксировать значение битовой вероятности ошибки (BER) обоих параллельных потоков. И после окончания исследования построить зависимости BER от SNR обоих параллельных потоков.

Содержание отчета

Титульный лист.

Цель работы.

Теория канала Downlink.

Исследуемая схема канала Downlink.

Результаты работы по пунктам 6 и 7.

Заключение.

В результате выполнения в разделе были выполнены следующие мероприятия:

Проведен теоритический анализ стандарта мобильной связи стандарта LTE. Проведен анализ сравнения данного стандарта с уже устаревающими стандартами на данный момент – UMTS (3G) и GSM (2G). Также было проведено аналитическое исследование физических каналов стандарта – Downlink (от БС к МС) и Uplink (от МС к БС), а также логические и транспортные каналы. Приведены обобщенные схемы формирования данных каналов.

Путем проведения компьютерной симуляции, была проверена достоверность теоритического исследования. В программе Matlab 15 были собрана схема канала Downlink.

С помощью компьютерной симуляции были получены различного рода зависимости при передаче информации по каналу. Самая важная из них это зависимость битовой вероятности ошибки от отношения сигнал/шум. В результате получились следующие значения:

Таблица 7.18. Зависимость BER от SNR при MIMO 4x4

сигнал/шум (дБ)	1 поток (BER)	2 поток (BER)
-15	0,4766	0,4537
-10	0,4347	0,3876
-5	0,3456	0,2729
1	0,1836	0,114
5	0,0774	0,039
10	0,0076	0,0027
15	0,000001	0,000002
20	0	0

25	0	0
30	0	0

Таблица 7.19. Зависимость BER от SNR при MIMO 2x2

сигнал/шум (дБ)	1 поток (BER)	2 поток (BER)
-15	0,4772	0,4645
-10	0,4354	0,4073
-5	0,3512	0,3096
1	0,2178	0,1933
5	0,1347	0,1345
10	0,056	0,074
15	0,0137	0,0282
20	0,0003	0,0037
25	0	0,000003
30	0	0

Анализируя полученные значения таблицы 3, можно сделать следующий вывод, что при увеличении отношения сигнал/шум, битовая вероятность ошибки стремится к нулю быстрее в MIMO 4x4, нежели в MIMO 2x2. Таким образом, использование большего числа приемо-передающих антенн, дает меньшие ошибки.

Была написана методика исследования канала Downlink.

Также я познакомился с различным программным обеспечением, для построения различного вида схем.

Подведя итог своего курсового проекта, можно сказать следующее, то, что я сделал, является основополагающим делом к дальнейшим, более трудным вещам. Курсовой проект был весьма увлекательным и полезным. С поставленными целями справился успешно.

8. Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем (задание на самостоятельную работу

Помехоустойчивое кодирование является эффективным способом оптимизации ТКС. На практике инженеру проектровщику ТКС приходится решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов. Решение именно такой задачи положено в основу СР.

Исходные данные заданы в таблице вариантов П1.2:

Цифровая информация передается двоичным кодом. Виды передаваемой цифровой информации:

ДК - данные компьютерного обмела;

ЦТЛФ - цифровая телефония;

ЦТВ - сообщения цифрового ТВ;

ЦЗВ - сообщения цифрового звукового вещания.

Канал святи - канал с постоянными параметрами и аддитивным белым гауссовым шумом.

Отношение с/ш на входе демодулятора $h_б = E_б / N_0$.

Методы модуляции: ФМ-2, ФМ-4.

Прием - когерентный.

Производительность источника $R_{ист}(бит/с)$.

Полоса пропускания канала $F_К(кГц)$.

Вероятность ошибки бита в сообщениях, отдаваемых получателю, не более р.

Допустимая сложность декодера СК (показатель сложности решетки кода) - не более W.

Необходимо:

Выбрать и обосновать выбор корректирующего кода для проектируемой ТКС, обеспечивающего требуемую вероятность ошибки бита р в сообщениях, отдаваемых получателю, при условии выполнения следующих ограничений:

Полоса частот кодированного сигнала не должна превышать полосу пропускания канала FK.

При использовании сверточных кодов показатель сложности решетки кода должен быть не более величины W.

Разработать и дать подробное описание структурной и функциональных схем кодера и декодера выбранного кода и обосновать их параметры.

Проанализировать показатели энергетической и частотной эффективности телекоммуникационной системы и сравнить их с предельными значениями эффективности.

4. Сделать заключение по выполненной работе.

Содержание пояснительной записки работы:

Задание и исходные данные.

Описание структурной схемы проектируемой телекоммуникационной системы с указанием мест включения кодера помехоустойчивого кода, модулятора, демодулятора и декодера с подробными пояснениями выполняемых ими функций.

Классификация корретирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в проекте сверточных кодов.

Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования СК.

Расчет ширины спектра цифрового сигнала с заданным видом модуляции.

Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода.

Определение допустимой скорости кода $R^*_{код}$ из условия непревышения полосой частот кодированного сигнала полосы пропускания канала (ограничение 1.1).

Определение перечня кодов со скоростями, превышающими допустимую скорость $R^*_{код}$, которые могут быть использованы для решения поставленной задачи.

Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита (условие 1) и удовлетворяющего требованию ограничения по сложности декодера (ограничение 1.2).

Проверочный расчет зависимости вероятности ошибки на выходе декодера выбранного СК.

Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК.

Заключение с подведением итогов выполненной работы.

Список использованных источников.

Методические указания к выполнению КР

Расчет ширины спектра сигнала ФМ-2 (ФМ-4) следует производить по рекомендациям материалов главы 1. Применение корректирующих кодов со скоростью $R^*_{код}$ приводит к

расширению спектра кодированного сигнала в $(K_F = 1/R_{КОД})$ раз. С другой стороны, корректирующая способность кода возрастает с уменьшением скорости кода (т.е. с увеличением избыточности). Поэтому задача оптимизации параметров корректирующего кода состоит в выборе кода со скоростью, при которой ширина спектра кодированного сигнала не превышает заданную полосу пропускания канала. Если требуемая полоса пропускания канала для передачи ФМ сигнала с информационной скоростью $R_{ИСТ}$ равна $F_{(ФМ)}$, а скорость кода выбрана равной $R_{КОД}$, то полоса пропускания канала, необходимая для передачи кодированного ФМ сигнала, будет равна

$$F_{К(ФМ-СК)} = \frac{F_{(ФМ)}}{R_{КОД}}.$$

Тогда из условия непревышения этой полосой частот сигнала полосы пропускания канала ($F_{К(ФМ-СК)} < F_К$) получаем простое условие для выбора скорости кода

$$R^*_{КОД} > R_{КОД} = \frac{F_{(ФМ)}}{F_К}. \qquad (П1.1)$$

Сказанное иллюстрируется рисунком 5.1. Ширина спектра кодированного ФМ сигнала пропорциональна коэффициенту расширения полосы. По мере снижения скорости кода (возрастания K_F) полоса расширяется и достигает значения полосы пропускания канала. На этом же рисунке показана зависимость АЭВК от K_F (что равноценно скорости кода). Пересечение кривой полосы с граничным заданным значением $F^*_К$ определяет допустимое значение коэффициента расширения полосы пропускания канала $K_p = 1/R_{КОД}$ и, соответственно, скорость кода $R^*_{КОД}$. Первым этапом выбора корректирующего кода.является выбор класса кодов (класс блоковых либо непрерывных (сверточных) кодов). Используя материалы разделов 8 и 11, рекомендуется аргументированно обосновать выбор класса сверточных кодов для применения в своей работе. Среди алгоритмов декодирования СК по широте практического применения лидирующее место занимает алгоритм Витерби. Рекомендуется в работе применить именно алгоритм Витерби. В разделе проекта с обоснованием применения этого алгоритма следует привести сведения о сложности реализации алгоритма. Среди кодов, отобранных по критерию скорости в соответствии с формулой (5.1), могут оказаться коды с различной длиной кодового ограничения (и, соответственно, с различной сложностью декодера). Помехоустойчивость декодирования СК характеризуется величиной ЭВК. В таблицах кодов не приводятся значения ЭВК при определенном уровне вероятности ошибки декодирования. В то же время, величина

асимптотического энергетического выигрыша (АЭВК) является верхней оценкой ЭВК. Поэтому при отборе кодов рекомендуется использовать величины АЭВК, значения которых имеются в таблицах приложения А. Среди отобранных кодов-кандидатов следует применить код, обеспечивающий максимальный АЭВК и удовлетворяющий требованиям по скорости и слоэ/сно- сти декодера. Окончательные данные о вероятности ошибки на выходе декодера следует получить на основе расчетов зависимости вероятности ошибки декодирования от отношения сигнал/шум для выбранного кода. В случае невыполнения требований задания рекомендуется применить код с большей величиной АЭВК.

Пример расчетов и процедуры оптимизации кода

Исходные данные:

1. Вид передаваемой цифровой информации - ЦТЛФ.

Отношение с/ш $h_б$ = 4 дБ.

Метод модуляции: ФМ-4.

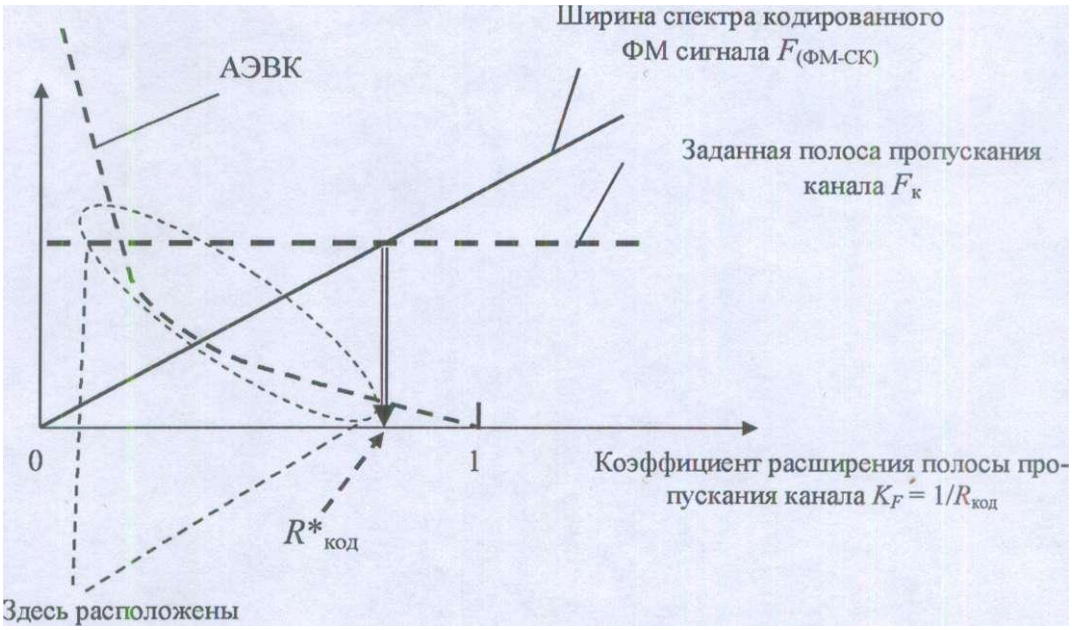
Прием-когерентный.

6. Производительность источника $R_{ИСТ}$ = 64 кбит/с

7. Ширина полосы частот канала FK= 100 кГц.

8. Допустимая вероятность ошибки бита p =10^{-5}.

9. Допустимая сложность решетки кода W = 150.



коды-кандидаты на выбор

Рис. 8.1. К процедуре оптимизации кода

Расчет полосы пропускания канала связи, необходимой для передачи цифровой информации с заданной скоростью методом ФМ-4, производим по формуле

$F_{(ФМ-4)} = [R_{ИСТ}(1-\alpha)]/2,$ где α - коэффициент ската спектра. Задаваясь значением α = 0,4, получаем $F_{(ФМ-4)} = [R_{ИСТ}(1-\alpha)]/2$ = [64(1 + 0,4)]/2 = 44,8 кГц.

В соответствии с формулой (5.1) определяем предельное значение скорости С К

$$R^*_{КОД} > \frac{F_{ФМ-СК}}{F_К} = \frac{44,8}{100} = 0,448.$$

3. По таблицам СК отбираем коды, удовлетворяющие требованию по скорости. Данные об этих кодах сведены в таб. 8.1.

Таблица 8.1. Характеристики СК для выбора кода

Скорость кода $R_{КОД}$	Порождающие многочлены	ДКО v	Сложность решетки W	АЭВК дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

Из таблицы видно, что для выполнения поставленной задачи могут быть использованы СК со скоростями $R_{КОД} = 1/2,$ которые обеспечивают достаточно большой АЭВК. На аснове данных таблицы выбираем для проекта код с порождающими многочленами (133, 171), который при скорости $R_{КОД} = 0,5$ обеспечивает АЭВК = 6,99 дБ. Данные расчета вероятности ошибки приведены в главе 1.

Видно, что применение выбраного кода обеспечивает выполнение задания: при отношении сигнал/шум $h_б^2 = 4$ дБ вероятность ошибки декодирования менее $3 \cdot 10^{-5}$ Сравнение с кривыми помехоустойчивости некодированной ФМ (рис. 11.1) показывает, что при вероятности ошибки $p = 10^{-5}$ этот код обеспечивает ЭВК 5,3 дБ.

Таблица 8.2. Исходные данные для выполнения СР

Номер варианта для выполнения СР должен соответствовать номеру фамилии студента в журнале академической группы

Номер варианта	Вид перед, информ.	Отношение С/Ш на входе $h_б^2$, *дБ*	Метод модул.	Производит. источника $R_{ИСТ}$, кбит/с	Полоса пропуск, канала FK, кГц	Вер. ошибки бита p	Сложи. декодера W
1	ДК	4,0	ФМ-4	64	80	10^{-6}	150
2	ЦТЛФ	5,0	ФМ-4	16	25	10^{-4}	160
3	ЦЗВ	6,0	ФМ-2	256	800	10^{-5}	170
4	ДК	6,5	ФМ-2	64	200	10^{-6}	180
5	ЦТЛФ	4,0	ФМ-4	16	25	10^{-4}	250
6	ЦЗВ	7,0	ФМ-4	128	200	10^{-5}	350
7	НТВ	5,0	ФМ-2	2400	7000	10^{-8}	560
8	ДК	6,0	ФМ-4	32	50	10^{-6}	200
9	ЦТЛФ	5,0	ФМ-2	24	70	10^{-4}	300
10	ЦЗВ	4,5	ФМ-4	256	400	10^{-5}	250
11	ЦТВ	5,5	ФМ-2	3000	1200	10^{-8}	550
12	ДК	4,0	ФМ-4	48	70	10^{-6}	150
13	ЦТЛФ	5,0	ФМ-4	32	50	10^{-4}	250
14	ЦЗВ	7,0	ФМ-2	256	800	10^{-5}	300
15	ЦТВ	4,0	ФМ-4	4500	1300	10^{-9}	550
16	ДК	7,0	ФМ-4	56	90	10^{-6}	150
17	ЦТЛФ	5,0	ФМ-2	24	70	10^{-4}	160
18	ЦЗВ	4,5	ФМ-4	256	400	10^{-5}	200
19	ЦТВ	5,5	ФМ-4	5000	1400	10^{-9}	550
20	ДК	6,0	ФМ-2	64	200	10^{-6}	150
21	ЦТЛФ	7,5	ФМ-4	256	400	10^{-4}	250
23	ЦЗВ	6,5	ФМ-4	16	50	10^{-5}	150
24	ДК	6,0	ФМ-4	64	150	10^{-6}	150
25	ЦГЛФ	4,5	ФМ-2	16	25	10^{-6}	200
26	ЦТВ	5,0	ФМ-2	6000	16000	10^{-9}	550
27	ЦЗВ	6,0	ФМ-4	384	600	10^{-5}	250

28	ДК	4,5	ФМ-4	64	100	10^{-6}	150
29	ЦГЛФ	5,0	ФМ-2	16	50	10^{-4}	250
30	ЦТВ	5,5	ФМ-2	5500	32000	10^{-9}	560
31	ЦГЛФ	4,5	ФМ-4	64	200	10^{-5}	150
32	ДК	5,0	ФМ-4	64	300	10^{-5}	250

Примеры расчетов для разных вариантов

Вариант №7

Таблица 8.3. Параметры проектируемой ТКС

Номер варианта для выполнения индивидуальной работы должен соответствовать номеру фамилии студента в журнале академической группы							
Номер варианта	Вид перед. Информации	Отношение С/Ш hб 2, дБ	Метод модуляции	Произв. источника Rист, кбит/с	Пропускная способность канала Fк, кГц	Вер. Ошибки бита	Сложн. декодера
7	ЦТВ	5.0	ФМ-2	2400	7000	10-8	560

Структурная схема проектируемой телекоммуникационной системы

В общем виде обобщенная структурная схема проектируемой ТКС может быть сформирована в виде, представленном на рисунке 8.1.

В передатчике кодер вносит в информационное сообщение избыточность в виде проверочных символов. Закодированные символы поступают на модулятор, который преобразует их в аналоговый сигнал.

В приемнике демодулятор преобразует принятый сигнал в последовательность чисел, представляющих оценку переданных данных – метрики. Метрики поступают в декодер, который исправляет возникающие при передаче ошибки, используя внесенную кодером избыточность.

Классификация корректирующих кодов

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления — корректирующие коды(коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

В общем виде классификация корректирующих кодов может быть представлена в следующем виде:

Блочные коды:

Линейные коды общего вида;

Коды Хемминга;

Линейные циклические коды:

Коды CRC;

Коды БЧХ;

Коды коррекции ошибок Рида — Соломона;

Сверточные коды;

Каскадные коды.

Стоит отметить, что блочные коды, как правило, хорошо справляются с редкими, но большими пачками ошибок, их эффективность при частых, но небольших ошибках (например, в канале с АБГШ), менее высока.

Вместе с этим, сверточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок.

Так как в начальных условиях поставленной задачи не были сформулированы требования к методам кодирования, выбор остановился на сверточных кодах. Однако, при проектировании телекоммуникационных систем необходимо четко формировать критерии оптимальности разрабатываемой системы.

Классификация методов декодирования сверточных кодов

Классификация методов декодирования сверточных кодов имеет следующий вид:

Алгебраические методы декодирования;

Вероятностные методы декодирования:

Алгоритм последовательного декодирования;

Алгоритм Витерби.

Алгоритм Витерби характеризуется постоянством вычислительной работы, однако сложность декодера Витерби растет, как при переборных алгоритмов, по экспоненциальному закону от длины кодового ограничения сверточного кода.

Так как в данной работе в целях оптимизации проектируемой системы будут использоваться короткие сверточные коды, сложность декодера будет мала, что позволяет использовать алгоритм декодирования Витерби.

Расчет и оптимазация параметров телекоммуникацонной системы

Расчет ширины спектра цифрового сигнала с заданным видом модуляции:

$$F_{ФМ-2} = \frac{R_{ист} \cdot (1+\alpha)}{2} = \frac{2400 \cdot 10^3 \cdot (1+0.4)}{2} = 1.68 МГц$$

.

Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода:

$$R_{код*} = \frac{F_{ФМ-2}}{F_к} = \frac{1680 \cdot 10^3}{7000 \cdot 10^3} = 0.24$$

.

Следовательно скорость кода должна быть не менее 0.24. Полученный результат позволяет сформировать список подходящих сверточных кодов в виде представленном в таблице 8.4.

Татлица 8.4. Перечень подходящих сверточных кодов

Скорость кода $R_{код}$	Порождающие многочлены	ДКО v	Сложность решетки W	АЭВК, дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

В силу того, критерием оптимальности проектируемой ТКС является простота используемого кодера/декодера, был выбран код /133,171/ с длиной кодового ограничения 7, который при скорости кода 0.5 обеспечивает АЭВК = 6.99 дБ.

Изложенное позволяет рассчитать ширину спектра кодированного цифрового сигнала:

$$F_{ФМ-2+СК} = \frac{F_{ФМ-2}}{R_{код}} = \frac{1680 \cdot 10^3}{0.5} = 3.36 МГц$$

Рисунок 6.2 позволяет сделать вывод о том, что применение выбранного кода обеспечивает выполнение поставленной задачи, так как при отношении С/Ш = 5 дБ вероятность ошибки декодирования меньше 10-5.

Сравнение с кривыми помехоустойчивости некодированной ФМ показывает, что при вероятности ошибки 10-8 этот код обеспечивает значение ЭВК более 10 дБ.

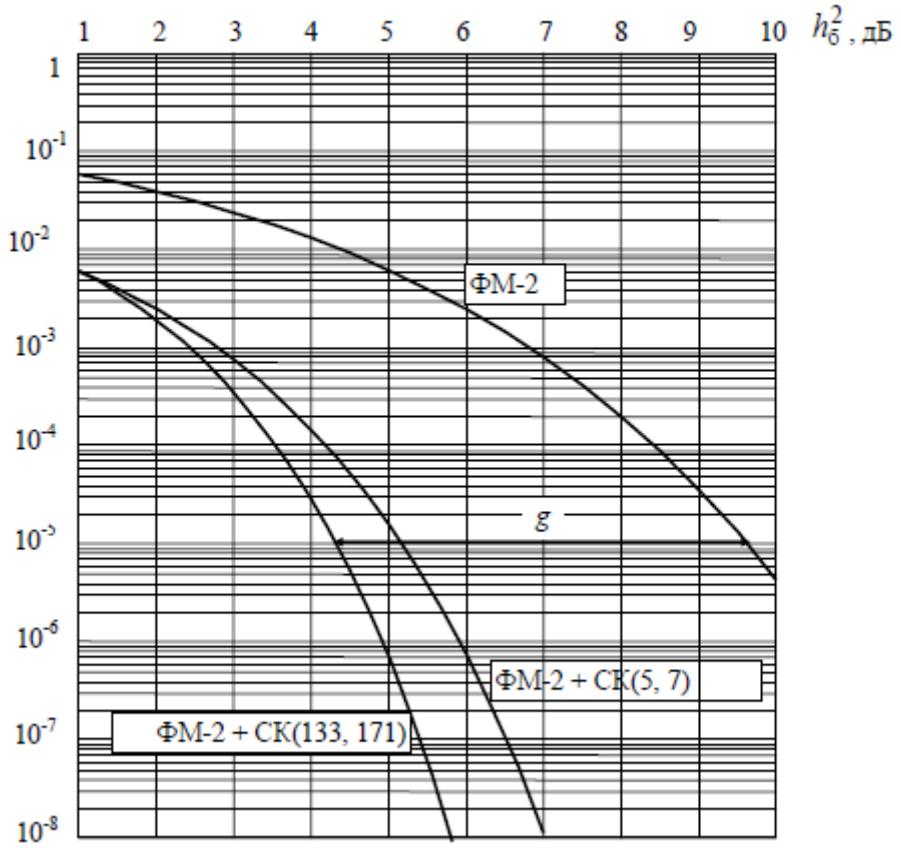


Рис. 8.2. Помехоустойчивость декодирования сверточных кодов

Проверочный расчет вероятности ошибки на выходе декодера:

$$Q = 0.65 \cdot \exp(-0.44 \cdot (z + 0.75)^2) = 0.65 \cdot$$

$$\cdot \exp(-0.44 \cdot (5.01 + 0.75)^2) = 2.972 \cdot 10^{-7}$$

$$p_д = w_{df} \cdot Q \cdot (\sqrt{2 \cdot d_f \cdot R_{код} \cdot h_б}) = 36 \cdot 2.972 \cdot 10^{-7} \cdot (\sqrt{2 \cdot 10 \cdot 0.5 \cdot 5}) = 7.565 \cdot 10^{-5}$$

Расчет показал, что реальное значение вероятности ошибки кодера меньше теоретического значения, следовательно, условия задачи были выполнены.

Разработка кодера и декодера сверточного кода 133,171

В предыдущем разделе был описан выбор сверточного кодера /133,171/. Функциональная и структура схема кодера/декодера может быть представлена в следующем виде:

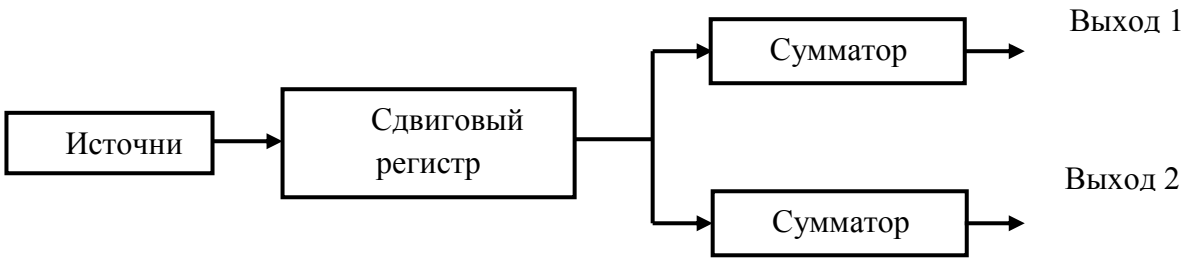


Рис. 8.3. Структурная схема сверточного кодера

1338 → 10110112

1718 → 11110012

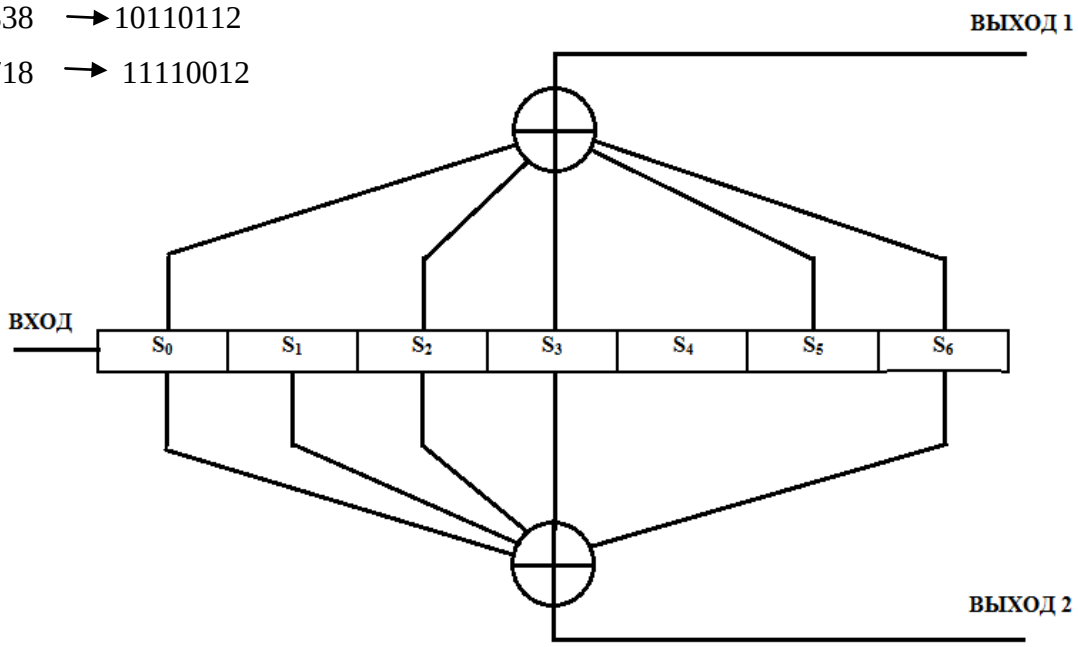


Рис. 8.4. Функциональная схема сверточного кодера 133,171

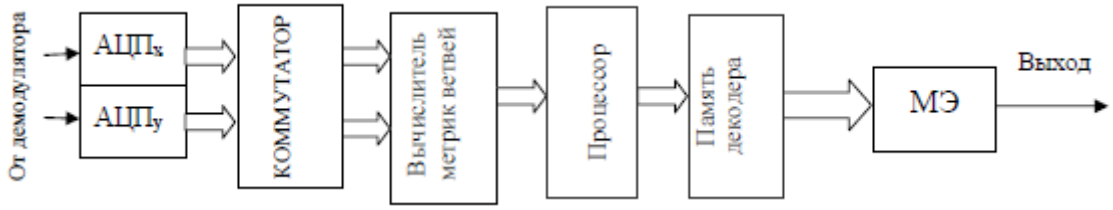


Рис. 8.5. Структурная схема декодера Витерби

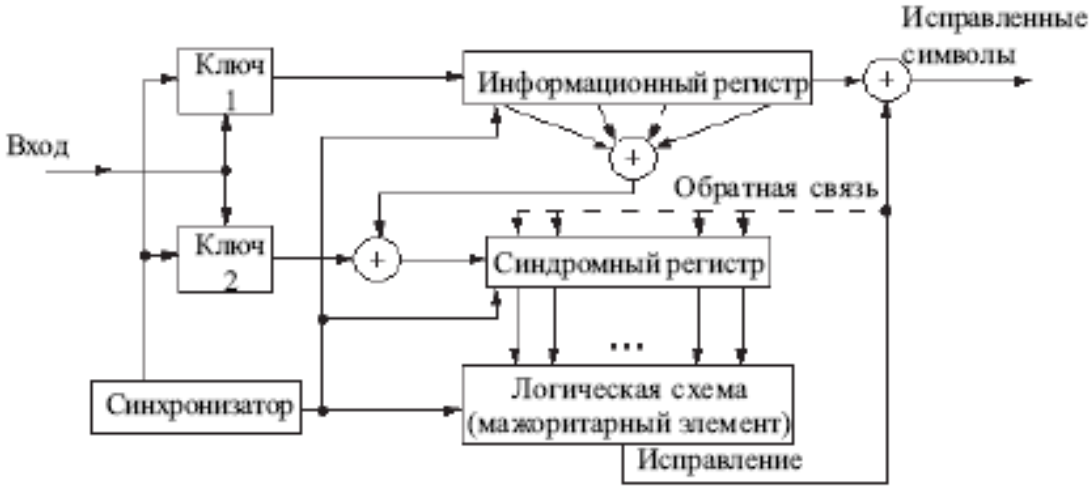


Рис. 8.6. Функциональная схема декодера Витерби

В результате выполнения данной индивидуальной работы было сделано следующее:

Спроектирована телекоммуникационная система с использованием сверточного кодера;

Рассчитаны и оптимизированы параметры сверточного кода используемого в ТКС в целях повышения ее эффективности и помехоустойчивости;

Предложены структурные и функциональные схемы кодера и кодера, используемых в разработанной ТКС.

Варианты № 16, 3, 8

Для решения поставленной задачи предложены общие параметры проектируемой ТКС, которые представленные в таблице 8.5.

Таблица 8.5. Параметры проектируемой ТКС

Номер варианта	Вид перед. инф-ии	Отношение С/Ш hб2, дБ	Метод модуляции	Произв. источника Rист, кбит/с	Пропускная способность канала Fк, кГц	Вер. ошибки бита p	Сложн. декодера W
16	ДК	7,0	ФМ-4	56	90	10-6	150
3	ЦЗВ	6,0	ФМ-2	256	800	10-5	170
8	ДК	6,0	ФМ-4	32	50	10-6	200

Структурная схема проектируемой телекоммуникационной системы

Структурная схема проектируемой телекоммуникационной системы представлена на рисунке 8.2.

Источник сообщения генерирует бинарную последовательность с определенной скоростью $R_{\text{ист}}$. Курсивом отмечены блоки, которые кодируют и декодируют информацию с применением помехоустойчивых кодов (вводится избыточность при кодировании, например код Хемминга, БЧХ, сверточный код). Что касается источника, то он кодируется и декодируется с помощью таких алгоритмов как, Хаффмана, Шеннона-Фано или Лемпела-Зива. В данных алгоритмах не вводится избыточность. Помимо кодирования система связи содержит в себе квадратурную модуляцию/демодуляцию. Где на выходе модулятора мы получаем сначала комплексные числа (квадратурные и синфазные составляющие), которые в свою очередь садятся на несущие, сдвинутые на 90 градусов и в конечном итоге суммируются. Демодуляция представляет собой обратный процесс. Варианты работы содержит в себе модуляцию ФМ-2 или BPSK, которая имеет только два синфазных значения постоянной амплитуды и фазы 0 и 180 градусов и ФМ-4 или QPSK, которая имеет четыре значения постоянной амплитуды и фазы. И, конечно же, любая система передачи не обходится без воздействия на нее шумов, в канале беспроводной сети (канал связи).

Классификация корректирующих кодов

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления — корректирующие коды(коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

Преимущества и недостатки блоковых кодов:

Блоковые коды, как правило, хорошо справляются с редкими, но большими пачками ошибок, их эффективность при частых, но небольших ошибках (например, в канале с АБГШ), менее высока.

Преимущества и недостатки свёрточных кодов:

Свёрточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок. Выбор в индивидуальной работе сверточных кодов обосновывается тем, что свёрточное кодирование - очень простая операция. Кодирование свёрточным кодом производится с помощью регистра сдвига, отводы от которого суммируются по модулю два. Таких сумм может быть две (чаще всего) или больше.

Классификация корректирующих кодов по структуре представлена на рисунке в.

Классификация методов декодирования сверточных кодов

Классификация методов декодирования сверточных кодов имеет следующий вид:

Алгебраические методы декодирования;

Вероятностные методы декодирования:

Алгоритм последовательного декодирования;

Алгоритм Витерби.

Задача декодирования сверточного кода заключается в выборе пути (в этом и состоит отличие декодирования сверточных кодов) вдоль решетки наиболее похожего на принятую последовательность. Каждый путь вдоль решетчатой диаграммы складывается из ветвей соединяющих узлы. Каждой ветви решетки соответствует кодовое слово из двух бит. Каждую ветвь на каждом периоде можно пометить расстоянием Хемминга между полученным кодовым словом и кодовым словом, соответствующим ветви. Складывая расстояния Хемминга ветвей, составляющих путь, получим метрику соответствующего пути. Данная метрика будет характеризовать степень подобия каждого пути принятой последовательности. Чем меньше метрика, тем более похожи путь и принятая

последовательность. Таким образом, результатом декодирования будет информационная последовательность, соответствующая пути с минимальной метрикой. Если в одно и тоже состояние входят два пути выбирается тот, который имеет лучшую метрику. Такой путь называется выжившим. Отбор выживших путей проводится для каждого состояния. Это не иначе как алгоритм декодирования Витерби и он наиболее эффективный.

Расчет ширины спектра цифрового сигнала с заданным видом модуляции

Вариант	Расчеты
16	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{56*(1+0,4)}{2} = 39,2$ кГц
3	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{256*(1+0,4)}{2} = 179,2$ кГц
8	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{32*(1+0,4)}{2} = 22,4$ кГц

Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала

Вариант	Расчеты
16	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0.436$
3	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0.224$
8	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0,448$

Определение кода

Полученный результат позволяет сформировать список подходящих сверточных кодов в виде, представленном в таблице 8.6.

Таблица 8.6. Характеристики СК для выбора кода

Скорость кода $R_{код}$	Порождающие многочлены	ДКО v	Сложность решетки W	АЭВК, дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

Вариант	Условия
16	СК со скоростями 1/2 и сложностью решетки W не более 150
3	Все СК со сложностью решетки W не более 170

8	СК со скоростями ½ и сложностью решетки W не более 200

Произведен выбор СК из перечня, обеспечивающего заданную вероятность ошибки бита и удовлетворяющего требованию ограничения по сложности декодера.

Вариант	Выбранный СК
16	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ
3	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ
8	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ

Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода

Вариант	Расчеты
16	$F_{ФМ4+СК} = \frac{F_{FM4}}{R_{код}} = \frac{39,2}{0,5} = 78,4$ кГц
3	$F_{FM2+СК} = \frac{F_{FM2}}{R_{код}} = \frac{179,2}{0,5} = 358,4$ кГц
8	$F_{ФМ4+СК} = \frac{F_{FM4}}{R_{код}} = \frac{22,4}{0,5} = 44,8$ кГц

Рисунок 8.7 позволяет сделать вывод о том, что применение выбранного кода обеспечивает выполнение поставленной задачи, так как

Вариант	Отношение С/Ш hб 2, дБ	Вероятность ошибки декодирования меньше
16	7,0	10-6
3	6,0	10-5
8	6,0	10-6

Сравнение с кривыми помехоустойчивости некодированной ФМ показывает, что

Вариант	Вероятность ошибки	АЭВК, дБ
16	10-6	более 10
3	10-5	9,4
8	10-6	более 10

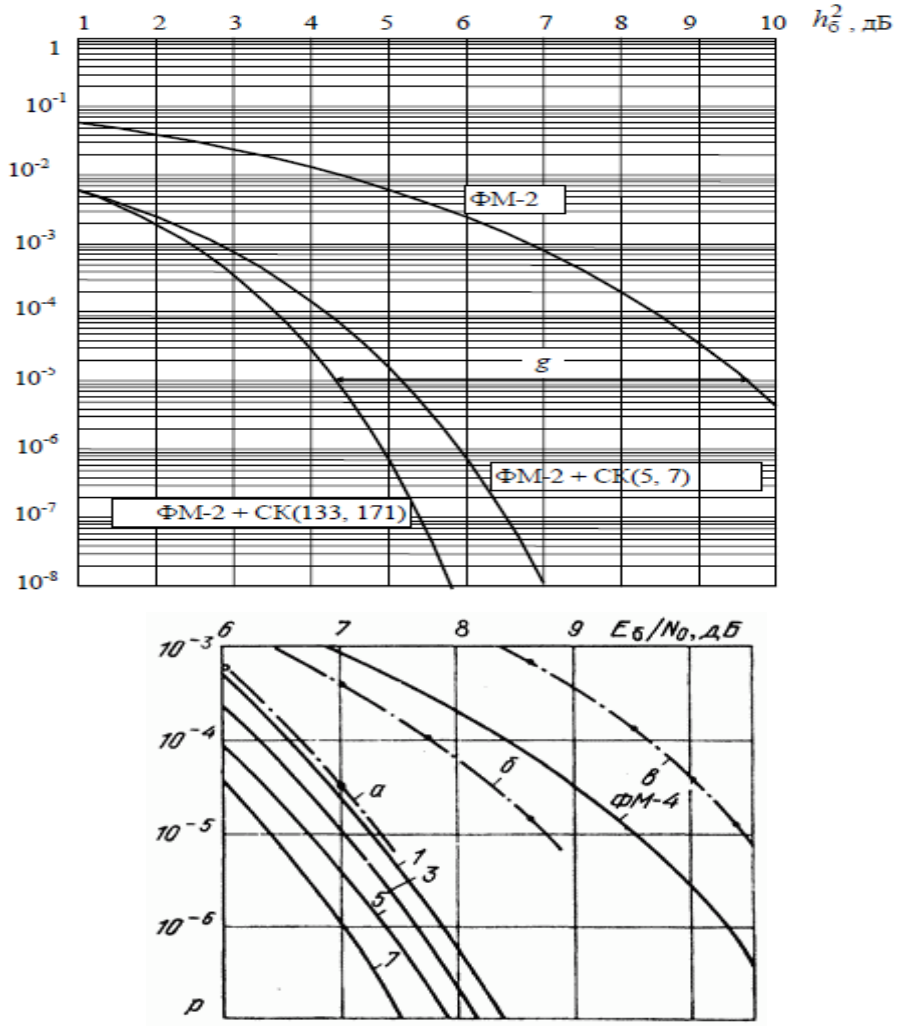


Рис. 8.7. Помехоустойчивость декодирования сверточных кодов

Проверочный расчет зависимости вероятности ошибки на выходе декодера

В результате получим (примерно для заданной вероятности ошибки бита):

Вариант	Расчеты
16	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{5{,}01 * \sqrt{2\pi}} * \exp\left(-\frac{5{,}01^2}{2}\right) = 4{,}45 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 4.45 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 7} = 4.2 \cdot 10^{-3}$
3	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{4 * \sqrt{2\pi}} * \exp\left(-\frac{4^2}{2}\right) = 3{,}3 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 3.3 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 6} = 9.2 \cdot 10^{-3}$
8	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{5{,}01 * \sqrt{2\pi}} * \exp\left(-\frac{5{,}01^2}{2}\right) = 4{,}45 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 4.45 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 6} = 4.2 \cdot 10^{-3}$

Расчет показал, что реальное значение вероятности ошибки кодера меньше теоретического значения, следовательно, условия задачи были выполнены.

Разработка кодера и декодера СК 133, 171

В предыдущем разделе был описан выбор сверточного кодера (133,171).

1338 = 10110112;1718 = 11110012

Функциональная и структура схема кодера/декодера может быть представлена в следующем виде:

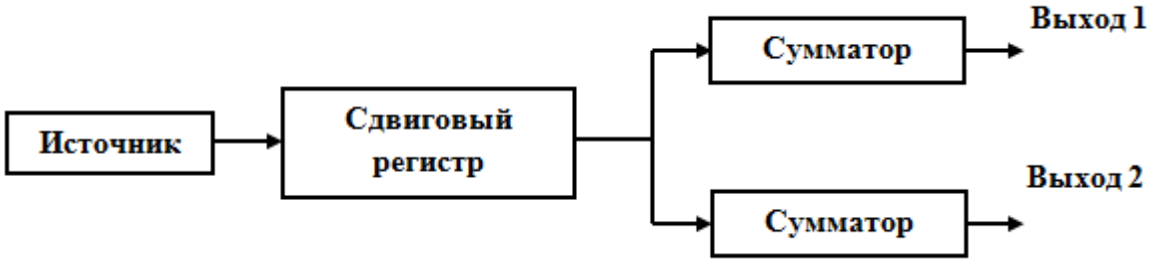


Рис. 8.8. Структурная схема сверточного кодера

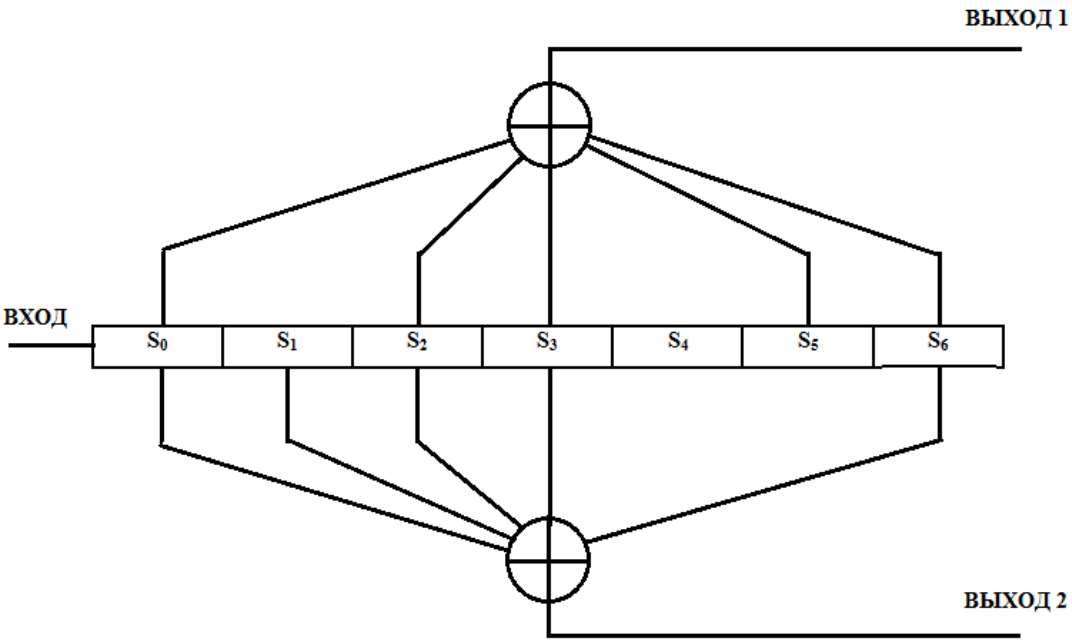


Рис. 8.9. Функциональная схема сверточного кодера 133,171

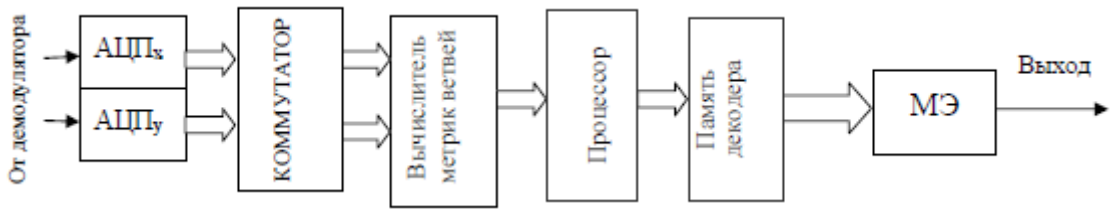


Рис. 8.10. Структурная схема декодера Витерби

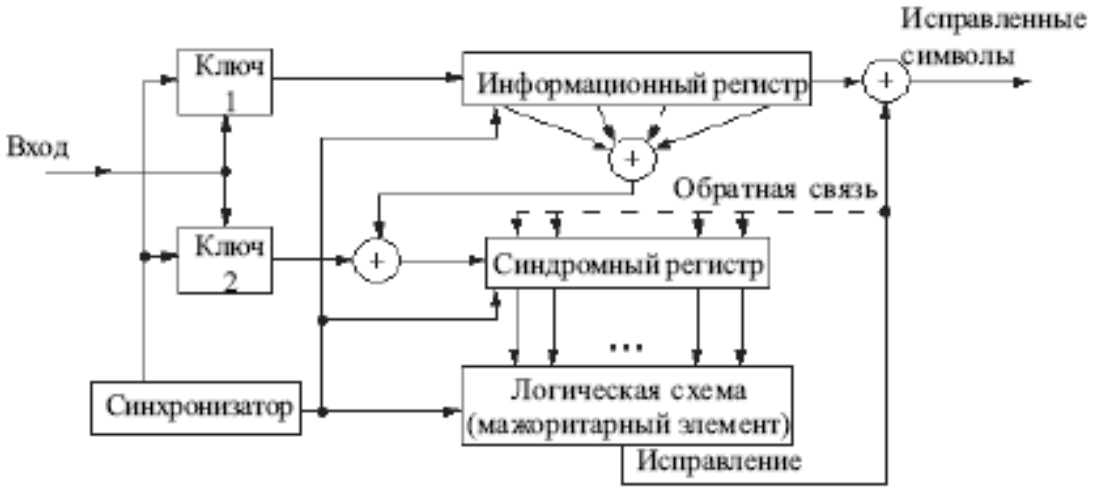


Рис. 8.11. Функциональная схема декодера Витерби

кодера со скоростью 1/2.

В результате выполнения данного индивидуального задания было выполнено следующее:

Спроектирована телекоммуникационная система с использованием сверточного кодера;

Рассчитаны и оптимизированы параметры сверточного кода используемого в ТКС в целях повышения ее эффективности и помехоустойчивости при различных начальных заданных условиях (ширина спектра, скорость кода, битовая вероятность ошибки в зависимости от заданного значения отношения сигнал/шум);

Предложены структурные и функциональные схемы кодера и кодера, используемых в разработанной ТКС.

ЗАКЛЮЧЕНИЕ

Сегодня Интернет не воспринимается как достаточно надежная сеть для передачи трафика реального времени. Но это происходит не из-за недостатка перспективных механизмов, таких как потоковые слежение и ограничение (shaping/policing), а из-за сложности выбора метода обеспечения QoS сети и компромисса между простотой и большей управляемостью. Хороший проект сети, простота, высокая доступность и обеспечение защиты являются ключевыми аспектами обеспечения QoS на магистралях Интернет. Хороший проект сети плюс некоторая степень резервирования ресурсов не только делают сеть более отказоустойчивой, но также и предотвращают многие проблемы, связанные с QoS, и устраняют потребность в сложных механизмах, разработанных для их решения. Это делает сеть более простой и увеличивает ее доступность. Три класса трафика (Premium, Assured, и Best effort) достаточны для удовлетворения обозримых потребностей клиентов. Различные классы трафика будут обслуживаться по-разному, особенно при неблагоприятных сетевых условиях. Быстрая перемаршрутизация MPLS или другие механизмы защиты могут

использоваться для защиты Premium-трафика при отказах маршрутизаторов или каналов. При возникновении неисправностей в одной части сети инжиниринг трафика должен использоваться для перемещения трафика в другую часть сети. DiffServ инжиниринг трафика может использоваться для предотвращения концентрации высокоприоритетного трафика на любом канале, так что высокопроизводительный трафик будет иметь низкую задержку и джиттер, и при необходимости может обрабатываться предпочтительно за счет трафика других классов. Схемы управления трафиком на магистрали, такие как Policing и Shaping, должны применяться для микроконтроля и использоваться, когда инжиниринг трафика становится недостаточным.

Проведено имитационное моделирование на базе MATLAB 2015b Simulink модемов и кодеков современных телекоммуникационных систем стандарта CDMA, системы мобильной связи стандарта IEEE 802.11 (WiFi), мобильной связи стандарта IEEE 802.15.4 ZigBee, системы мобильной связи стандарта IEEE 802.15.1 (Bluetooth), системы мобильной связи стандарта IEEE 802.16 (WiMAX), системы мобильной связи стандарта IEEE 802. 20 LTE. Получены основные характеристики ТКС в зависимости от параметров систем, характеристик сигналов и влияния шумов и многолучевости (для CDMA). Представлены созвездия для модуляторов, спектры сигналов на входе и выходе канов связи, а также Зависимости вероятности битовой ошибки от отношения сигнал/шум и многолучевости.

Материалы учебного пособия могут быть использованы как для учебных целелей, так и как справочный материал при проектировании ТКС.

ЛИТЕРАТУРА

1. Пакетная сеть связи общего пользования. Кучерявый А.Е., Гильченок Л.З., Иванов А.Ю. - СПб.: НкТ, 2004.
2. Телекоммуникационные системы и сети: Учебное пособие. В 3 т. Том 1: Современные технологии / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов; под ред. проф. В.П. Шувалова. - 3-е изд., испр. и доп. - М.: Горячая линия - Телеком, 2003. - 647 с.
3. Телекоммуникационные системы и сети_ Учебное пособие. В 3 т. Том 3 - Мультисервисные сети. В. В. Величко, Е. А. Субботин, В. П. Шувалов, А. Ф. Ярославцев. М.: Горячая линия – Телеком, 2005. – 592 с.
4. Банкет В.Л. Помехоустойчивое кодирование в телекоммуникационных системах: учебн. пособие. - Одесса: ОНАС им А.С. Попова, 2011. - 104 с.
5. Зюко А.Г., Фалько А.И., Панфилов И.П., Банкет В.Л., Иващенко П.В. Помехоустойчивость и эффективность систем передачи информации. М.:Радио и связь. 1985.

6. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи: учеб. пособие / В. А. Варгаузин, И. А. Цикин. — СПб.: БХВ-Петербург, 2013. — 352 с.
7. Банкет В.Л. Сигнально-кодовые конструкции в телекоммуникационных системах. - Одесса: Фешкс, 2009. - 180 с.
8. Мелихов С.В. Аналоговое и цифровое радиовещание: Учебное пособие. Издание второе, исправленное. - Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2012. – 233 с.
9. Голиков А.М., Уваровский В.Д. Исследование многоуровневых методов модуляции сигналов, используемых в космических системах связи, на базе аппаратуры и ПО labVIEW 2010. Методические указания по лабораторным работам – Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2011. – 50 с.
10. Галкин В.А. Цифровая мобильная радиосвязь. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2007. – 432 с..
11. Федосов В. П., Нестеренко А. К. Цифровая обработка сигналов в LabVIEW: учеб. пособие / под ред. В. П. Федосова. – М.: ДМК Пресс, 2007. – 456 с.
12. Теория и техника передачи информации : учебное пособие /Ю. П. Акулиничев, А. С. Бернгардт. — Томск: Эль Контент, 2012. — 210 с.
13. Скляр Б. Цифровая связь. — М.: Издательский дом Вильямс. 2003 — 1104с
14. Феер К.: Беспроводная цифровая связь. М.: Радио и связь, 2000. - 520 с.
15. Крейнделин В.Б., Колесников А.В. Оценивание параметров канала в системах связи с ортогональным частотным мультиплексированием. Учебное пособие / МТУСИ.-М., 2010. -29 с.
16. Д. Ватолин, М. Смирнов «Методы сжатия данных: Сжатие изображений» // http://www.compression.ru/book/part2/part2__3.htm
17. С. Уэлстид. “Фракталы и вейвлеты для сжатия изображений в действии”. Москва. “Издательство ТРИУМФ” 2003. 360 .
18. https://sites.google.com/site/szatieinformacii/lekcii/tema13
19. Дворкович В.П., Дворкович А.В. Цифровые видеоинформационные системы (теория и практика) Москва: техносфера, 2012. – 1008 с.
20. LabVIEW. Справочник по функциям. [Электронный ресурс]. – Режим доступа:http://chaos.sgu.ru/library/programms/progr/ labVIEW/LabVIEW_suranov.pdf
21. Майков, Д.Ю. Оценка сдвига частоты для процедуры Initial Ranging в системе «мобильный WiMax» / Д.Ю. Майков, А.Я. Демидов, Н.А. Каратаева, Е.П. Ворошилин // Доклады ТУСУРа. – 2011. – №2 (24). – 59-63 с.

22. Серов А. В. Эфирное цифровое телевидение DVB-T/H. - БХВ-Петербург, 2010. – 465 с.

23. Стандарт DVB-H. Система мобильного ТВ вещания. [Электронный ресурс] – Режим доступа: http://www.konturm.ru/tech.php?id=dvbh

24. http://www.mathworks.com/examples/simulink-communications/mw/comm_product-LTEDownlinkExample-lte-phy-downlink-with-spatial-multiplexing

25. J. H. Yuen, et. al. Modulation and Coding for Satellite and Space Communications. Proc. IEEE,vol. 78., n. 7, July, 1990, pp. 1250-1265.

26. Forney G. Concatenated Codes. Cambridge, Massachusetts: M. I. T. Press, 1966.