РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук

**К. Е. Самуйлов, Д. С. Кулябов, А. В. Королькова,
Ю. В. Гайдамака, И. А. Гудкова, П. О. Абаев**

Современные концепции управления инфокоммуникациями

Учебно-методический комплекс

Москва
Российский университета дружбы народов
2013

УДК 004.72, 004.057.4
ББК
С

Утверждено
РИСО Учёного совета
Российского университета
дружбы народов

Издание подготовлено в рамках реализации
Программы стратегического развития РУДН на 2012–2016 гг.

Самуйлов К. Е.

С Современные концепции управления инфокоммуникациями [Текст] / К. Е. Самуйлов, Д. С. Кулябов, А. В. Королькова, Ю. В. Гайдамака, И. А. Гудкова, П. О. Абаев. — М. : РУДН, 2013. — 235 с. : ил.

Учебное-методический комплекс обеспечивает реализацию программы дисциплины «Современные концепции управления инфокоммуникациями» и предназначен для студентов, обучающихся на магистерской программе «Управление инфокоммуникациями и интеллектуальные системы» по направлению «Фундаментальная информатика и информационные технологии». Комплекс содержит учебное пособие «Архитектура и принципы построения сетей связи следующих поколений».

ISBN

Описание курса и программа

«Современные концепции управления инфокоммуникациями»

Описание курса

Цели и задачи курса

Область знаний

Курс относится к области знаний «Информационно-телекоммуникационные системы», соответствующей одноименному приоритетному направлению развития науки и технологий, входящему в перечень, утвержденный Президентом Российской федерации.

Уровень обучения и направления подготовки по действующему перечню

Курс является частью магистерской программы «Управление инфокоммуникациями и интеллектуальные системы» направления 010300 «Фундаментальная информатика и информационные технологии».

Согласно учебному плану курс является дисциплиной по выбору вариативной части общенаучного цикла.

Цели курса

- Ввести учащихся в предметную область существующих систем и сетей инфокоммуникаций.
- Сформировать понятийный аппарат в области концепций, архитектур, стандартов современных систем и сетей инфокоммуникаций.
- Ознакомить слушателей с новыми технологиями в области систем и сетей инфокоммуникаций.
- Создать у слушателей понимание принципов построения современных систем и сетей инфокоммуникаций.

Задачи курса

После успешного прохождения курса слушатели должны:

знать:

- базовые понятия систем и сетей инфокоммуникаций;
- общие характеристики концепций, архитектур, стандартов современных систем и сетей инфокоммуникаций;
- основные принципы управления современными системами и сетями инфокоммуникаций;
- современные концепции управления инфокоммуникациями в области концепций, архитектур, моделей и методов управления инфокоммуникациями

уметь:

- осуществлять анализ принципов построения архитектур сетей IP и мультисервисных сетей следующего поколения;
- анализировать принципы построения, архитектур и методологий систем управления инфокоммуникациями.

владеть:

- навыками и подходами в области анализа и построения архитектур, моделей и методов управления инфокоммуникациями.

Инновационность курса

По содержанию.

Современные методы проектирования сетей и систем инфокоммуникаций в частности базируются на новейших достижениях целого ряда научных областей, обеспечивающих развитие приоритетного направления развития науки и технологий – информационно-телекоммуникационные технологии, – входящего в перечень, утвержденного Президентом Российской федерации. К этим областям в первую очередь относятся информационная интеграция, информационно-телекоммуникационные системы и искусственный интеллект. Последние достижения в этой области сконцентрированы в целом ряде концепций, архитектурных моделей и методологий, принятых на международном уровне в виде стандартов и рекомендаций, разработанных ведущими производителями и исследовательскими центрами. Эти концепции в свою очередь опираются на другие новейшие достижения в области инфокоммуникационных технологий.

Содержание курса обеспечивает слушателей необходимым объёмом знаний для освоения основ построения и эксплуатации современных сетей и систем инфокоммуникаций.

По методике преподавания и организации учебного процесса.

Методика преподавания основана на применении современных информационных технологий. Учебно-методический комплекс с «Архитектура и принципы построения современных сетей и систем телекоммуникаций» помимо традиционных методических материалов включает электронный учебник, интегрированный в инфокоммуникационную среду типа. Эти средства позволяют организовать и провести лабораторные занятия в виде виртуального класса, где студенты работают под руководством преподавателя в асинхронном режиме. Такой режим позволяет осуществлять эффективный контроль уровня знаний за счет постоянного наблюдения за степенью освоения курса учащимися и за ходом выполнения промежуточных видов контроля знаний.

По литературе.

В настоящее время основная масса литературных источников описывает предметную область либо слишком абстрактно, либо углубляясь в несущественные детали. Учебная литература на русском языке по большей части

потеряла актуальность и содержит устаревшие данные. Современное состояние предметной области доступно в основном в литературе на иностранных языках (английском).

По организации учебного процесса.

Учебный процесс реализуется в соответствии с философией педагогики социального конструкционизма и ориентирован прежде всего на организацию взаимодействия между преподавателем и студентами. Учебный процесс интегрирован с компьютерными комплексами поддержки обучения. Также в учебном процессе используются интерактивные формы обучения.

Сведения об авторах

Самуйлов Константин Евгеньевич

Доктор технических наук, профессор, заведующий кафедрой систем телекоммуникаций РУДН.

Родился 17 августа 1955 года. Окончил в 1978 г. Университет дружбы народов им. П. Лумумбы, по специальности математик, в дипломной работе исследовал методы расчета характеристик сетей массового обслуживания. В 1985 г. защитил кандидатскую диссертацию «Системы массового обслуживания ограниченной емкости и их приложение к анализу информационно-вычислительных систем» на факультете Вычислительной математики и кибернетики МГУ им. М.В. Ломоносова по специальности 01.01.05 «Теория вероятностей и математическая статистика». В 2005 году защитил докторскую диссертацию «Методы анализа и расчета сетей сигнализации и мультисервисных сетей с одноадресными и многоадресными соединениями» в Московском техническом университете связи и информатики по специальности 05.12.13 «Системы, сети и устройства телекоммуникаций».

Член рабочей группы «Интеллектуальные сети» Международной федерации по обработке информации (IFIP), постоянный член программных комитетов 3-х международных конференций, в 1997 - 1999 гг. член Российской делегации 11-ой Исследовательской комиссии Международного союза электросвязи, член-корреспондент Международной академии информатизации, в 1998-2000 гг. визитный профессор в Технологическом университете г. Хельсинки, в 2001-2002 гг. - в Технологическом университете г. Лаппеенранта, Финляндия. Руководитель ряда проектов реализованных для ОАО «Ростелеком», ОАО «Центртелеком», ОАО «Уралсвязьинформ», ОАО «МТС», ОАО «МТТ», ОАО «МГТС», ОАО «Гипросвязь», ЗАО «Коминфо Консалтинг», Telecom Finland и Sonera, Nokia, Ericsson и др.

Ведет активные научные исследования и разработки в области проектирования сетей связи следующего поколения (NGN), систем поддержки операционной и бизнес-деятельности компаний связи (NGOSS/ BSS), математической теории телетрафика мультисервисных сетей. Автор более 100 научных работ и 2-х монографий в области теории телетрафика, математических методов анализа и расчета цифровых сетей связи, методов анализа и расчета показателей качества мультисервисных сетей.

Основные публикации:

1. Martikainen O., Naoumov V., Samouylov K. Call Processing Model for Multimedia Services // Intelligent Networks and New Technologies (Villy B. Iversen and Jorgen Norgaard eds), Chapman & Hall, London, 1996, pp. 241–251.
2. Martikainen O., Naoumov V., Samouylov K., Zhidovinov M. A Framework of Service Components Modeling for Multimedia Distribution over Broadband Network // Intelligent Networks and Intelligence in Networks (Dominique Gaiti ed.). - Chapman & Hall, London, 1997, pp. 115–127.
3. Martikainen O., Naoumov V., Samouylov K. Telecommunication Signalling// Wiley Encyclopedia of Electrical and Electronics Engineering. V. 21 (John.G. Webster, Editor). - John Wiley & Sons, 1999, pp. 426–432.
4. Samouylov K. Inconsistency between Q.706 and E.733 and queuing delay calculations in Q.706. // COM11-D1479 ITU-T SG11. - Geneva, November-December, 1999, 9 p.
5. Chukarin A., Samouylov K. Tool for the Routing Planning in a Large-scale Signaling Network // Proc. of the 7th Int. Conf. on Telecommunications, ConTEL 2003, Zagreb. - June 2001, pp. 579–586.
6. Самуйлов К.Е., Полищук В.П., Чукарин А.В. Схема сети ОКС-7 Московской области // Вестник связи. - 2002. - No10, С. 80–86.
7. Самуйлов К.Е. Методы анализа и расчета сетей ОКС 7. Монография // М. Изд-во РУДН, 2002. - 291 с.
8. Аджемов А.С., Самуйлов К.Е.и др. Принципы построения сети ОКС 7 на ЕСЭ Российской Федерации. Монография. // М. Изд. ФГУП ЦНИИС, 2004. - 246 с.
9. Савчук А.С., Самуйлов К.Е., Чукарин А.В. О стандартизации бизнес процессов для компаний отрасли связи // Электросвязь, No 6, 2006. - С. 19–26.
10. Наумов В.А., Самуйлов К.Е., Яркина Н.В. Теория телетрафика мультисервисных сетей: Монография. // М.: Изд-во РУДН, 2007. - 191 с.
11. Башарин Г.П. , Гайдамака Ю.В., Самуйлов К.Е., Яркина Н.В. Управление качеством и вероятностные модели функционирования сетей связи следующего поколения. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15144 от 11.02.2009, номер гос. регистрации 0320802917
12. Башарин Г.П., Гайдамака Ю.В., Самуйлов К.Е., Яркина Н.В. Модели для анализа качества обслуживания в сетях связи следующего поколения. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15157 от 10.02.2009, номер гос. регистрации 0320802930
13. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Введение в управление инфокоммуникациями. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15189 от 11.02.2009, номер гос. регистрации 0320802962
14. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Единая информационная модель управления инфокоммуникационной компанией. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15142 от 11.02.2009, номер гос. регистрации 0320802915

15. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Основы управления инфокоммуникационными компаниями. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15159 от 10.02.2009, номер гос. регистрации 0320802932
16. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Основы формальных методов описания бизнес-процессов. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15156 от 10.02.2009, номер гос. регистрации 0320802929
17. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Расширенная карта процессов деятельности телекоммуникационной компании. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15141от 11.02.2009, номер гос. регистрации 0320802914
18. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Системы следующего поколения для поддержки операционной деятельности инфокоммуникационной компании. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15143 от 11.02.2009, номер гос. регистрации 0320802916
19. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Современные концепции управления инфокоммуникациями. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15139 от 11.02.2009, номер гос. регистрации 0320802912
20. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Формальные языки моделирования процессов деятельности инфокоммуникационных компаний. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15140 от 11.02.2009, номер гос. регистрации 0320802913
21. Ромашкова О.Н., Самуйлов К.Е., Чащин А.А. О стандартизации архитектурных решений для предоставления услуг IPTV // Документальная электросвязь. - М., Ноябрь 2008, С. 19-24
22. Гайдамака Ю.В., Зарипова Э.Р., Самуйлов К.Е. Модели обслуживания вызовов в сети сотовой подвижной связи. Учебно-метод. пособие. Москва, РУДН, 2008. – 72 с. (эл. Вид)
23. Башарин Г.П., Самуйлов К.Е., Яркина Н.В., Гудкова И.А. Новый этап развития математической теории телетрафика // Автоматика и телемеханика, No 12. - Академиздатцентр «Наука» РАН, С. 16–28
24. Кулябов Д.С., Ловецкий К.П., Самуйлов К.Е., Севастьянов Л.А., Хохлов А.А. Инновационная магистерская программа «Математическое моделирование оптических наноструктур»/ IV Международная научно - практическая конференция «Современные информационные технологии и ИТ - образование», - тезисы докладов. - Москва, ВМК МГУ, С. 163–171
25. Самуйлов К.Е., Чукарин А.В., Яркина Н.В. Бизнес-процессы и информационные технологии в управлении телекоммуникационными компаниями. - М.: Альпина Паблишерз. - 2009. - 442 с. (монография)
26. Лузгачев М.В., Самуйлов К.Е. Задача маршрутизации трафика на графе сети MPLS с одноадресными соединениями // Вестник РУДН. Серия «Математика. Информатика. Физика». No 1, 2009. - С. 23–33

27. Першаков Н. В., Самуйлов К. Е. Системы M |G|1 с групповым обслуживанием и их применение к анализу модели протокола управления потоковой передачей. Часть I // Вестник РУДН. Серия «Математика. Информатика. Физика». No 1, 2009. - С. 34–44
28. Першаков Н. В., Самуйлов К. Е. Системы M |G|1 с групповым обслуживанием и их применение к анализу модели протокола управления потоковой передачей. Часть II // Вестник РУДН. Серия «Математика. Информатика. Физика». No 2, 2009. - С. 43–53
29. Гайдамака Ю.В., Гудкова И.А., Самуйлов К.Е. Приближенный анализ марковской модели звена сети Triple Play // International Workshop DISTRIBUTED COMPUTER AND COMMUNICATION NETWORKS (DCCN-2010), Proceedings, Moscow, Russia, October 26-28, 2010 M.: R&D Company Information and Networking Technologies. - 2010. С. 6–10
30. Лузгачев М. В., Самуйлов К. Е. Метод решения задачи разделения ресурсов мультисервисной сети между виртуальными частными сетями с одноадресными и многоадресными соединениями // Вестник Российского университета дружбы народов, серия «Математика. Информатика. Физика». - №2, вып. 1. - 2010. - С. 42–53
31. Лузгачев М.В., Самуйлов К.Е. The Resource Allocation Problem in the Design of Virtual Private Networks with Unicast and Multicast Connections // Proc. of the IEEE International Conference on Ultra Modern Telecommunications ICUMT 2010. Moscow, Russia – P. 1096–1101
32. Нсангу М.М., Самуйлов К.Е. Анализ модели сервера в сети NGN// International Workshop Distributed Computer and Communication Networks (DCCN-2010), Proceedings, Moscow, Russia, October 26-28, 2010 - M.: R&D Company Information and Networking Technologies. - 2010. С. 124–129
33. Нсангу Мушили, Самуйлов К.Е., Сопин Э.С. Модель функционирования сервера присутствия в сети NGN // T-Comm Телекоммуникации и транспорт №7. - 2010. - С.116–118
34. Нсангу Мушили, Самуйлов К.Е., Чукарин А.В Построение и анализ Марковской модели установления соединения по протоколу SIP с учетом повторных передач // T-Comm Телекоммуникации и транспорт №7, 2010. - С.139–141
35. Самуйлов К.Е., Сопин Э.С., Чукарин А.В. Оценка характеристик сигнального трафика в сети связи на базе подсистемы IMS // "T-Comm — Telecommunications and Transport" magazine, 2010, №7. - С. 8-13
36. Абаев П.О., Гайдамака Ю.В., Самуйлов К.Е. Гистерезисное управление сигнальной нагрузкой в сети SIP-серверов // Вестник РУДН. Серия «Математика. Информатика. Физика», № 4. М.: РУДН. - 2011. -С. 55–73.
37. Самуйлов К.Е., Сопин Э.С К анализу методов балансировки нагрузки несущей в системах LTE ADVANCED // T-Comm – Телекоммуникации и Транспорт. - № 7. М.: ИД «Медиа Паблишер». - 2011. - С. 136–139
38. Самуйлов К.Е., Чукарин А.В., Быков С.Ю. Основы формальных методов описания бизнес-процессов : Учебное пособие. М.: Изд-во РУДН, 2011. - 123 с.
39. Abaev P., Gaidamaka Yu., Samouylov K. Modeling of Hysteretic Signaling

Load Control in Next Generation Networks // Lecture Notes in Computer Science Vol. 7469. — 2012. — P. 44-452
40. Abaev P., Gaidamaka Yu., Samouylov K. Queuing Model for Loss-Based Overload Control in a SIP Server Using a Hysteretic Technique // Lecture Notes in Computer Science Vol. 7469. — 2012. — P. 371–378

Кулябов Дмитрий Сергеевич

Доцент кафедры систем телекоммуникаций РУДН, кандидат физико-математических наук, доцент. Начальник сектора системного администрирования отдела ИЕТФ УИ РУДН.

Родился 22 апреля 1970 года. Окончил в 1994 году бакалавриат Университета дружбы народов им. П. Лумумбы, по специальности физика, в выпускной работе исследовал солитонные решения уравнения Деви-Стюарта. В 1996 году окончил магистратуру Университета дружбы народов им. П. Лумумбы, по специальности физика, в магистерской диссертации исследовал устойчивость самогравитирующих солитонов. В 2000 году защитил кандидатскую диссертацию «Приложение лоренцовых 2-спиноров к некоторым проблемам теории поля» на факультете ФМИЕН РУДН по специальности 01.04.02 «Теоретическая физика». С 1996 по 2000 годы работал в НИИГазпром. Ведёт активные научные исследования и разработки в области проектирования IP-сетей, операционных систем, информационной безопасности. Автор более 30 научных работ в области сетевых технологий, информационной безопасности, операционных систем.

Основные публикации:

1. Самуйлов К. Е., Кулябов Д. С. Учебно-методическое пособие по курсу «Сети и системы телекоммуникаций». — М.: Изд-во РУДН, 2002. — 55 с.
2. Королькова А. В., Кулябов Д. С. Инфраструктура открытых ключей // Вестник РУДН, серия «Прикладная и компьютерная математика». — Т.2, №2. — 2003. — С. 123–151.
3. Королькова А. В., Кулябов Д. С. Необходимость обеспечения безопасности операционных систем на системном уровне // Вестник РУДН, серия «Прикладная и компьютерная математика». — Т. 3, №1. — 2004.— С. 144–161.
4. Королькова А. В., Кулябов Д. С. Адаптация системы работы с файлами устройств для SELinux // Вестник Российского университета дружбы народов, серия «Прикладная и компьютерная математика». Т. 4, №1. — 2005. — С. 153–163.
5. Кулябов Д.С., Ланеев Д.Е. Моделирование динамики взаимодействия WEB-сервера и пула клиентов в компьютерной сети в условиях атаки «Отказ в обслуживании» // Вестник Российского университета дружбы народов, серия «Прикладная и компьютерная математика». — Т. 4, №1. — 2005.— С. 164–178.
6. Кулябов Д. С., Королькова А.В., Хохлов А.А. Подсистема маршрутизации Click // Вестник Российского университета дружбы народов, серия «Математика. Информатика». — Т. 1, №12. — 2007.

7. Королькова А.В., Кулябов Д.С., Черноиванов А.И. К вопросу о классификации алгоритмов RED // Вестник РУДН, серия «Математика. Информатика. Физика», No 3, 2009. — С. 34–46
8. Кулябов Д. С., Королькова А. В. Архитектура и принципы построения современных сетей и систем телекоммуникаций. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15192 от 12.02.2009, номер гос. регистрации 0320802965
9. Кулябов Д. С., Королькова А. В. Введение в формальные методы описания бизнес-процессов. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15188 от 11.02.2009, номер гос. Регистрации 0320802961
10. Кулябов Д.С., Ловецкий К.П., Самуйлов К.Е., Севастьянов Л.А., Хохлов А.А. Инновационная магистерская программа «Математическое моделирование оптических наноструктур»/ IV Международная научно — практическая конференция «Современные информационные технологии и ИТ - образование», — тезисы докладов. — Москва, ВМК МГУ, С. 163–171
11. Королькова А. В., Кулябов Д. С. Математическая модель динамики поведения параметров систем типа RED // Вестник Российского университета дружбы народов, серия «Математика. Информатика. Физика». — №2, вып. 1. — 2010. — С. 54–64
12. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Курс лекций. — Учебное пособие, 2012. — 146 с.
13. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Лабораторные работы. — Учебное пособие, 2012. — 135 с.
14. Кулябов Д. С., Королькова А. В., Зарядов И. С. Обзор подходов к моделированию модуля управления трафиком // T-Comm - Телекоммуникации и транспорт. — 2012. — № 7. — С. 122–125.

Королькова Анна Владиславовна

Кандидат физико-математических наук, доцент кафедры систем телекоммуникаций РУДН.

Родилась 22 мая 1981 года. В 2003 году окончила бакалавриат РУДН, а в 2005 году - магистратуру РУДН по направлению «Прикладная математика и информатика», магистерская диссертация была посвящена вопросу построения защищённой системы на базе SELinux.

С 2005 по 2009 года обучалась в аспирантуре на кафедре систем телекоммуникаций по специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ». В 2010 г. защитила диссертацию «Математическая модель процесса передачи трафика с регулируемой алгоритмом типа RED динамической интенсивностью потока» на соискание ученой степени кандидата физико-математических наук.

С 2007 года по настоящее время работает на кафедре систем телекоммуникаций РУДН, с июля 2011 г. — в должности доцента. С 2002 года по настоящее время также работает в секторе системного администрирования отдела ИЕТФ УИТО РУДН.

Автор более 20 научных работ в области сетевых технологий, информационной безопасности, математического и имитационного моделирования.

Основные публикации:

1. Королькова А.В., Кулябов Д.С. Инфраструктура открытых ключей// Вестник РУДН, серия «Прикладная и компьютерная математика». — Т.2, №2. — 2003. — С. 123–151.
2. Королькова А.В., Кулябов Д.С. Необходимость обеспечения безопасности операционных систем на системном уровне // Вестник РУДН, серия «Прикладная и компьютерная математика». — Т. 3, №1. — 2004. — С. 144–161.
3. Королькова А.В., Кулябов Д.С. Адаптация системы работы с файлами устройств для SELinux // Вестник РУДН, серия «Прикладная и компьютерная математика». — Т. 4, №1. — 2005. — С. 153–163.
4. Королькова А.В. Метод расчета вероятности сброса пакетов в алгоритме RED // Вестник РУДН, серия «Математика. Информатика. Физика». — Т. 1, №12. — 2007.
5. Кулябов Д.С., Королькова А.В., Хохлов А.А. Подсистема маршрутизации Click // Вестник РУДН, серия «Математика. Информатика. Физика». — Т. 1, №12. — 2007.
6. Королькова А.В., Кулябов Д.С. Инструментальные средства моделирования DiffServ // Фундаментальные физико-математические проблемы и моделирование технико-технологических систем.— Вып. 11 / Под редакцией Л.А. Уваровой. М.: Издательство «Янус-К», 2008. — С. 161–167
7. Королькова А.В., Кулябов Д.С., Геворкян М.Н. Разработка модулей Click, реализующих алгоритмы активного управления очередью DSRED и SDRED // Моделирование нелинейных процессов и систем.- М.: МГУП, 2008. — С. 181–182.
8. Королькова А.В., Кулябов Д.С., Черноиванов А.И. К вопросу о классификации алгоритмов RED // Вестник РУДН, серия «Математика. Информатика. Физика», No 3, 2009. — С. 34–46
9. Кулябов Д. С., Королькова А. В. Архитектура и принципы построения современных сетей и систем телекоммуникаций. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15192 от 12.02.2009, номер гос. регистрации 0320802965
10. Кулябов Д. С., Королькова А. В. Введение в формальные методы описания бизнес-процессов. Уч. пособие, электронное издание на CD / Регистрационное свидетельство No 15188 от 11.02.2009, номер гос. регистрации 0320802961
11. Королькова А. В. Определение области возникновения автоколебаний в системах типа RED // Вестник РУДН, серия «Математика. Информатика. Физика», No 1, 2010. — С. 110–112
12. Королькова А. В., Кулябов Д. С. Математическая модель динамики поведения параметров систем типа RED // Вестник РУДН, серия «Математика. Информатика. Физика», No 2(1), 2010. — С. 54–64
13. Королькова А. В. Математическая модель процесса передачи трафика с регулируемой алгоритмом типа RED динамической интенсивностью потока

/ Дис.... канд. физ.-математ. наук: 05.13.18 Москва, 2010. — 115 с.
14. Королькова А. В., Черноиванов А.И. Использование СДУ для моделирования поведения TCP-трафика при взаимодействии с узлом, работающим по алгоритму RED. Определение области возникновения автоколебаний на примере алгоритмов RED, ARED, RARED, POWARED // «Математика. Компьютер. Образование». Сб. научных трудов/ Под редакцией Г.Ю. Ризниченко. — Т. 1 М.-Ижевск: НИЦ "Регулярная и хаотическая динамика", 2010. — С. 270–282
15. Korolkova A.V., Zaryadov I.S. The Mathematical Model of the Traffic Transfer Process with a Rate Adjustable by RED "2010 International Congress on Ultra Modern Telecommunications and Control Systems. (ICUMT 2010)" and Workshops Proceedings 18–20 Oct. 2010 Moscow, Russia IEEE P. 1046—1050.
16. Королькова А., Черноиванов А. Модификация модели процесса передачи с регулированием алгоритмом типа RED интенсивности потока для случая TCP-NewReno трафика // International Workshop "DISTRIBUTED COMPUTER AND COMMUNICATION NETWORKS (DCCN-2010)", Proceedings, Moscow, Russia, October 26-28, 2010. — M.: R&D Company "Information and Networking Technologies". — 2010. — С. 262–267
17. Зарядов И. С., Королькова А. В. Модель расчета показателей RED-подобных алгоритмов с помощью систем с групповым входящим потоком // International Workshop "Distributed computer and communication networks (DCCN-2011)" M.: R&D Company "Information and Networking Technologies". — 2011. — С. 65–72
18. Зарядов И. С., Королькова А. В., Разумчик Р.В. Математические модели расчета и анализа характеристик систем активного управления очередями с двумя входящими потоками и различными приоритетами // T-Comm - Телекоммуникации и транспорт. — 2012. — No 7. — С. 107–111.
19. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Курс лекций. — Учебное пособие, 2012. — 146 с.
20. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Лабораторные работы. — Учебное пособие, 2012. — 135 с.
21. Кулябов Д. С., Королькова А. В., Зарядов И. С. Обзор подходов к моделированию модуля управления трафиком // T-Comm - Телекоммуникации и транспорт. — 2012. — № 7. — С. 122–125.

Гайдамака Юлия Васильевна

Кандидат физико-математических наук, доцент, доцент кафедры систем телекоммуникаций РУДН.

В 1995 году окончила магистратуру Российского университета дружбы народов, факультет физико-математических и естественных наук по специальности «Прикладная математика и информатика», в 2001 году окончила очную аспирантуру и защитила диссертацию «Анализ вероятностно-временных характеристик звена сети передачи данных» на соискание ученой степени кандидата физико-математических наук по специальности 05.13.17 «Теоретические основы информатики». С мая 2003 г. - доцент кафедры систем телекоммуникаций физико-математического факультета РУДН.

Основные публикации:

1. Gaidamaka Y.V., Samouilov K.E. SS7 signaling link delays in the extreme error condition // Proc. of the 2-nd Int. Conf. IN-2000, October 17-19, 2000.- Moscow, Russia.- 2000.- P.29/1-29/10.
2. Жарков М.А., Гайдамака Ю.В., Самуйлов К.Е. К расчету задержек в звене сигнализации ОКС 7 при базовом методе защиты от ошибок // Электросвязь. -2000.- №3.- С.30-34.
3. Гайдамака Ю.В., Першаков Н.В., Чукарин А.В. Модель протокола SCTP и ее применение к анализу характеристик сигнального трафика при передаче по IP-сетям // Электросвязь. - 2007.- №9.- С.4-8.
4. Андрианов Г.А., Самуйлов К.Е., Гайдамака Ю.В. Анализ модели трафика ОКС 7 по результатам обработки статистики измерений // Вестник связи. -2007. - №11. - С.17-23.
5. Летников А.И., Пшеничников А.П., Гайдамака Ю.В., Чукарин А.В. Системы сигнализации сетей с коммутацией каналов и коммутацией пакетов: Учебное пособие // М.: Изд-во МТУСИ, 2008. - 195 с.
6. Гайдамака Ю.В., Зарипова Э.Р., Самуйлов К.Е. Модели обслуживания вызовов в сети сотовой подвижной связи: Учебно-метод. пособие. – М.: Изд-во РУДН, 2008. – 72 с.: ил.
7. Г.П. Башарин, Ю.В. Гайдамака, К.Е. Самуйлов, Н.В. Яркина. Модели для анализа качества обслуживания в сетях связи следующего поколения. Уч. пособие. Москва, ИПК РУДН, 2008, 111 с.
8. Г.П. Башарин, Ю.В. Гайдамака, К.Е. Самуйлов, Н.В. Яркина. Управление качеством и вероятностные модели функционирования сетей связи следующего поколения. Уч. пособие. Москва, ИПК РУДН, 2008, 131 с.
9. Abaev P., Gaidamaka Yu., Samouylov K. Modeling of Hysteretic Signaling Load Control in Next Generation Networks // Lecture Notes in Computer Science Vol. 7469. — 2012. — P. 44-452
10. Abaev P., Gaidamaka Yu., Samouylov K. Queuing Model for Loss-Based Overload Control in a SIP Server Using a Hysteretic Technique // Lecture Notes in Computer Science Vol. 7469. — 2012. — P. 371–378
11. Гайдамака Ю.В., Гудкова И.А., Медведева Е.Г. К анализу схем повторного использования частот в беспроводной сети OFDMA // T-Comm – Телекоммуникации и Транспорт. № 7. — 2012. — С. 55–59

Абаев Павел Ованесович

Кандидат физико-математических наук, доцент кафедры систем телекоммуникаций РУДН.

В 2006 году окончил бакалавриат РУДН, а в 2008 году – магистратуру РУДН на кафедре систем телекоммуникаций под руководством д.т.н., проф. Самуйлова К.Е. Магистерская диссертация была посвящена разработке методов расчета характеристик функционирования беспроводных сетей связи третьего поколения. В 2011 г. закончил обучение в аспирантуре и защитил кандидатскую диссертацию на кафедре систем телекоммуникаций по специальности 05.13.17 «Теоретические основы информатики».

С 2005 по 2007 гг. работал инженером в отделе ИЕТФ УИ РУДН, с 2007 го-

да по настоящее время работает на кафедре систем телекоммуникаций. Ведет научные исследования и разработки в области проектирования сетей связи следующего поколения, математических методов анализа и расчета цифровых сетей связи и математической теории телетрафика. Участвовал в проектах, реализованных для ОАО «МГТС» и ЗАО «НТЦ АССНАЗ».

Основные публикации:

1. Абаев П.О., Гайдамака Ю.В., Рудикова Е.В. Численный анализ модели обслуживания сессий в сети GSM/GPRS. // T Comm Телекоммуникации и транспорт, No 7, 2010.
2. Абаев П.О., Хатунцев А.Б. Построение и анализ модели установления соединения по протоколу SIP в сети связи следующего поколения. // T Comm Телекоммуникации и транспорт, No 7, 2010.
3. Абаев П.О., Хатунцев А.Б. Модель расчета вероятностно-временных характеристик установления соединений в гибридных сетях связи. // Электросвязь, No 10, 2010.
4. On SIP Session Setup Delay Modeling in Next Generation Networks // Сборник трудов конференции International Congress on Ultra Modern Telecommunications and Control System (ICUMT 2010) and Workshops Proceedings Москва, 2010.
5. Abaev P., Gaidamaka Yu., Samouylov K. Modeling of Hysteretic Signaling Load Control in Next Generation Networks // Lecture Notes in Computer Science Vol. 7469. — 2012. — P. 44-452
6. Abaev P., Gaidamaka Yu., Samouylov K. Queuing Model for Loss-Based Overload Control in a SIP Server Using a Hysteretic Technique // Lecture Notes in Computer Science Vol. 7469. — 2012. — P. 371–378

Гудкова Ирина Андреевна

Кандидат физико-математических наук, доцент кафедры систем телекоммуникаций РУДН.

В 2007 г. окончила бакалавриат Российского университета дружбы народов по специальности «Прикладная математика и информатика». В 2009 г. в РУДН получила степень магистра прикладной математики и информатики по специализации «Программное обеспечение вычислительных сетей». В 2011 г. закончила аспирантуру и защитила кандидатскую диссертацию на кафедре систем телекоммуникаций по специальности 05.13.17 «Теоретические основы информатики» под научным руководством д.т.н., профессора Самуйлова К.Е.

С 2008 г. работает на кафедре систем телекоммуникаций. Ведет научные исследования и разработки в области математической теории телетрафика мультисервисных сетей, а также сигнализации в сетях связи следующего поколения.

Основные публикации:

1. Gudkova I.A. and Samouylov K.E. Approximating performance measures of a triple play loss network model // Lecture Notes in Computer Science, NEW2AN/ruSMART-2011, S. Balandin et al. (eds.). – Germany, Heidelberg, Springer-Verlag. – 2011. – Vol. 6869. – P. 360–369.

2. Гайдамака Ю.В., Гудкова И.А., Самуйлов К.Е. Приближенный анализ марковской модели звена сети Triple Play // Distributed Computer and Communication networks. Theory and Applications DCCN-2010. – Moscow, R&D Company «Information and Networking Technologies», 2010. С. 6–10.
3. Samouylov K.E. and Gudkova I.A. Recursive computation for a multi-rate model with elastic traffic and minimum rate guarantees // Proc. of the International Congress on Ultra Modern Telecommunications and Control Systems ICUMT-2010 (18–20 October 2010). – P. 1065–1072.
4. Gudkova I.A. and Plaksina O.N. Performance measures computation for a single link loss net-work with unicast and multicast traffics // Lecture Notes in Computer Science, NEW2AN/ruSMART-2010, S. Balandin, R. Dunaytsev, Y. Koucheryavy, (eds.). – Germany, Heidelberg, Springer-Verlag. – 2010. – Vol. 6294. – P. 256–265.
5. Гудкова И.А., Лузгачев М.В. Модели разделения ресурсов звена мультисервисной сети с эластичным трафиком // T-Comm – Телекоммуникации и Транспорт. – М.: Издательский дом Медиа Паблишер. – 2010. – № 7. – С. 22–24.
6. Башарин Г.П., Самуйлов К.Е., Яркина Н.В., Гудкова И.А. Новый этап развития математической теории телетрафика // Автоматика и телемеханика. – М.: Академиздатцентр «Наука» РАН. – 2009. – № 12. – С. 16–28.
7. Самуйлов К.Е., Яркина Н.В., Гудкова И.А. Математическая модель управления доступом в сетях Triple Play // IV международная конференция по проблемам управления МКПУ-IV (26–30 января 2009 г.): Сборник трудов. – М.: РАН ИПУ им. В.А. Трапезникова РАН. – 2009. – С. 1722–1730.
8. Самуйлов К.Е., Першаков Н.В., Гудкова И.А. Построение и анализ моделей системы с групповым обслуживанием заявок // Вестник РУДН. Серия «Математика. Информатика. Физика». – М.: РУДН. – 2007. – № 3–4. – С. 45–52.
9. Гайдамака Ю.В., Гудкова И.А., Медведева Е.Г. К анализу схем повторного использования частот в беспроводной сети OFDMA // T-Comm – Телекоммуникации и Транспорт. № 7. — 2012. — С. 55–59

Структура курса

Трудоемкость курса: 4 кредита (144 часа).
Аудиторные занятия:

лекции – 1 час в неделю (18 часов);
лабораторные занятия – 1 час в неделю (18 часов);

Самостоятельная работа студента: 6 часов в неделю (108 часов).

Содержание курса, объём знаний, общие требования к промежуточному и итоговому контролю знаний определяются программой курса, график обучения определяется календарным планом, а оценка освоения программы курса студентом – методикой оценки уровня знаний.

Требования к контролю знаний

В процессе чтения курса предусмотрены два промежуточных контроля знаний и итоговый контроль знаний. Оценка знаний студента по каждому виду контроля осуществляется в соответствии с методикой оценки знаний.

Промежуточный контроль знаний № 1.

Контроль уровня знаний осуществляется в форме теста.

Примерные тестовые задания по дисциплине представлены ниже.

1. Дерево доставки отличается от дерева кратчайших путей тем, что оно:
   (a) Не всегда определяет кратчайший путь доставки
   (b) Доступно только узлам, запрашивающим пакеты
   (c) Строится динамически
   (d) Обеспечивает эффективную доставку
2. Лавинный алгоритм (Flooding) не позволяет:
   (a) Построить дерево доставки
   (b) Осуществлять доставку группового трафика
   (c) Обеспечивать доставку дейтаграмм между соседними маршрутизаторами
   (d) Устранять проблему дублирования дейтаграмм
3. Основным достоинством алгоритма RPB заключается в том, что:
   (a) Он требует, чтобы маршрутизаторы владели информацией обо всем остовом дереве
   (b) Он не подразумевает специальных механизмов остановки процесса передачи
   (c) Он создает дерево доставки частично
   (d) Он может работать без протокола IGMP
4. Какой из следующих алгоритмов является самым эффективным для групповой доставки?
   (a) RPM
   (b) RPB
   (c) TRPB
   (d) Spanning Tree
5. В алгоритме CBT сообщение от маршрутизатора в направлении ядра для первоначального соединения называется:
   (a) JOIN ACK
   (b) JOIN REQUEST
   (c) ECHO REQUEST
   (d) ECHO REPLY
6. В алгоритме формирования дерева на основе ядра (CBT) родительским называется интерфейс по направлению:
   (a) От ядра к члену группы
   (b) От маршрутизатора к члену группы
   (c) От члена группы к ядру
   (d) От члена группы к узловому маршрутизатору
7. Что является самым большим недостатком протокола DVMRP?

(a) Недостаточная масштабируемость
(b) Порождение регулярных всплесков служебного трафика
(c) Генерация небольшого объема служебной информации
(d) Неполное соответствие стандартным нормам

8. Какое из следующих утверждений неверно?
(a) Сообщения IGMP передаются в IP дейтаграммах
(b) Хост отправляет первый IGMP отчет, когда первый процесс вступает в группу
(c) IGMP имеет сообщение фиксированного размера
(d) В качестве ”ведущего” выбирается маршрутизатор с наибольшим IP-адресом

9. По умолчанию значение 1 для TTL групповых дейтаграмм позволяет дейтаграмму распространяться:
(a) Только в своей подсети
(b) Только по всей сети
(c) По распределенной сети
(d) Между соседними маршрутизаторами

10. Какой из следующих элементов не входит в модель IP-мультивещания поверх ATM - RFC 2022 ?
(a) Сервер разрешения адресов мультивещания (MARS)
(b) Клиенты сервера MARS
(c) Сервер мультивещания(MSC)
(d) Абстрактный групповой ATM-адрес

11. Технология LANE не обеспечивает:
(a) Пакетирование и передачу данных
(b) Распознавание адресов
(c) Управление групповой рассылкой сообщений
(d) Выбор лучшей таблицы маршрутизации при любой передачи

12. Метод двунаправленного туннелирования используется:
(a) При удаленной подписке
(b) В алгоритме CBT
(c) В протоколе MoM
(d) В сетях с неподвижными узлами

13. Основным отличием протокола MMA от MoM является использование:
(a) Агентов
(b) Перенаправителей
(c) Метода туннелирования
(d) Дерева доставки

14. Протокол IGMP используется для:
(a) Управления группой
(b) Одноадресной передаче данных
(c) Управления маршрутизацией
(d) Построения дерева доставки

15. Протокол TRPB предложен вместо RPB, чтобы решить проблему:
(a) Вычисления самого короткого пути
(b) Определения отправителя сообщения

(c) Порождения ненужного трафика в подсети, не содержащей получателей
(d) Определения получателя сообщения

16. Протоколы IGMP, DVMRP, MOSPF, PIM:
(a) Взаимозаменяемы
(b) Являются протоколами управления группой
(c) Являются протоколами многоадресной маршрутизации
(d) Работают с протоколом передачи данных IP

17. Сколько основных видов PIM (Protocol Independent Multicast) имеется?
(a) 1 (один)
(b) 2 (два)
(c) 3 (три)
(d) 4 (четыре)

18. Какой из следующих принципов не применим к классификации протоколов групповой маршрутизации?
(a) Требуемый протокол класса IGP (EGP)
(b) Алгоритм построения деревьев доставки
(c) Применение на прикладном уровне
(d) Оптимальные условия доставки

19. Сколько RP алгоритмов (по обратному пути) применяются в данный момент?
(a) 1(один)
(b) 2(два)
(c) 3(три)
(d) 4(четыре)

20. Какое из следующих понятий не характерно для протокола BGMP?
(a) Домен
(b) Корневой домен
(c) Информационная база маршрутизации
(d) Точка встречи (Rendezvous Point)

Кроме того, контроль уровня знаний включает в себя результаты защиты рефератов по тематике содержания курсов. Написание рефератов осуществляется во время самостоятельных занятий. Лучшие рефераты представляются студентами в виде презентаций и обсуждаются на занятиях.

Примерные темы рефератов для самостоятельных занятий:

Тема 1. Технология Wi-Fi.

В реферате должен быть дан обзор стандартов технологии Wi-Fi, рассмотрена область применимости, приведена номенклатура производимого клиентского и коммутационного оборудования Wi-Fi.

Тема 2. Технология WiMAX.

В реферате должен быть дан обзор стандартов технологии WiMAX, рассмотрена область применимости, перспективы развития технологии WiMAX.

Тема 3. Технология ISDN.

В реферате должен быть дан обзор стандартов технологии ISDN, отражено современное состояние технологии ISDN. Кроме того, необходимо от-

ветить на вопрос «что позаимствовали из технологии ISDN другие технологии?».

*Тема 4.*Технология ATM.

В реферате должен быть дан обзор стандартов технологии ATM, проанализированы причины коммерческой неудачи ATM. Кроме того, необходимо ответить на вопрос «что позаимствовали из технологии ATM другие технологии?».

*Тема 5.*Технология GPRS.

В реферате должен быть дан обзор стандартов технологии GPRS, указаны причины возникновения и коммерческого успеха технологии GPRS, проанализированы причины отказа от GPRS и перехода на другие более современные технологии.

*Тема 6.*Статическая маршрутизация.

В реферате должны быть даны общие понятия маршрутизации, указаны области применения статической маршрутизации, описаны возможности расширенного управления IP-трафиком посредством статической маршрутизации. Кроме того, должны быть приведены примеры на базе Cisco, Linux (iproute2, click).

*Тема 7.*Динамическая маршрутизация.

В реферате должны быть даны общие понятия маршрутизации, указаны области применения динамической маршрутизации, классифицированы алгоритмы динамической маршрутизации. Кроме того, должны быть приведены конкретные примеры протоколов для каждого алгоритма динамической маршрутизации, их достоинства и недостатки, примеры на базе Cisco.

*Тема 8.*Коммутация в ATM и MPLS.

В реферате должны быть отражены причины возникновения технологий ATM и MPLS, области их применимости, приведены примеры удачного и неудачного внедрения данных технологий.

*Тема 9.*Softswitch и IMS.

В реферате должен быть дан обзор стандартов и протоколов технологий Softswitch и IMS, отражено различие в концепциях.

*Тема 10.*Основные протоколы стека H.323.

В реферате должен быть дан обзор стандартов, основных протоколов стека H.323, сферы применения. Кроме того, должен быть описан механизм соединения в рамках стека H.323, проведено сравнение с другими стеками протоколов.

Итоговый контроль знаний.

Контроль уровня знаний осуществляется в виде письменной контрольной работы.

Примерный перечень вопросов:

1. Технология MPLS.
2. Уровневое построение сети NGN.
3. Протоколы сигнализации в сетях с коммутацией пакетов.
4. Управление инфокоммуникациями по концепции TMN.

5. Уровневое представление сети телекоммуникаций – управление, сигнализация, соединения, транспорт.

Литература

Обязательная

1. Таненбаум Э. Компьютерные сети (3 или 4 изд.) // Спб.: Изд-во «Питер», 2007. – 992 с.
2. Самуйлов К.Е. Методы анализа и расчета сетей ОКС7 // М. Изд-во РУДН, 2002
3. Кулябов Д.С., Королькова А.В. Архитектура и принципы построения современных сетей и систем телекоммуникаций Уч. пособие // Москва, Изд-во РУДН, 2008
4. В. Вишневский, С. Портной, И. Шахнович Энциклопедия WiMAX. Путь к 4G, 2010
5. Х. Кааранен, А. Ахтиайнен, Л. Лаитинен, Сети UMTS. Архитектура, мобильность, сервисы, 2007
6. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH. — СПб.: БХВ. — Санкт-Петербург, 2006. — 368 с.
7. Гольдштейн Б.С. Интеллектуальные сети. Издательство: Радио и связь, 2000.

Дополнительная литература

1. Гольдштейн Б.С. Телекоммуникационные протоколы. Протоколы стека ОКС7: подсистема МАР. Кн. 10,2012
2. Jesse Russell W-CDMA (UMTS), 2012
3. Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский Сети связи, 2011
4. Gottfried Punz Evolution of 3G Networks: The Concept, Architecture and Realization of Mobile Networks Beyond UMTS, 2010
5. Б. С. Гольдштейн, А. А. Зарубин, В. В. Саморезов Протокол SIP. Справочник, 2005
6. Наумов В.А., Самуйлов К.Е., Яркина Н.В. Теория телетрафика мультисервисных сетей. - М.: Изд-во РУДН, 2007. - 191 с.
7. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. — М.: Издательский дом ”Вильямс”, 2004. — 304 с.
8. Вишневский В., Ляхов А., Портной С, Шахнович И. Широкополосные беспроводные сети передачи информации. — М.: Эко-Трендз, 2005. — 592 с.
9. Гулевич Д. С. Сети связи следующего поколения. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий. ИНТУИТ.ру, 2007.

Программа дисциплины

Цели и задачи дисциплины:

Основной целью курса является введение учащихся в предметную область современных концепций и архитектур управления телекоммуникациями:

- сформировать понятийный аппарат в области концепций, архитектур, моделей и методов управления инфокоммуникациями.
- создать у слушателей понимание базовых методологий построения систем управления инфокоммуникационными компаниями.

В процессе преподавания курса решаются следующие задачи:

- анализ принципов построения архитектур сетей IP и мультисервисных сетей следующего поколения.
- анализ принципов построения, архитектур и методологий систем управления инфокоммуникациями.

Место дисциплины в структуре ООП:

Цикл, к которому относится дисциплина: вариативная часть общенаучного цикла М.1. Дисциплины по выбору студента

Требования к входным знаниям и умениям: профессиональные компетенции по направлениям 010400 ”Прикладная математика и информатика” (бакалавриат). 010300 «Фундаментальная информатика и информационные технологии» (бакалавриат), 010200 «Математика и компьютерные науки» (бакалавриат), 080500 Бизнес-информатика.

Дисциплины, для которых данная дисциплина является предшествующей: Современные концепции инфокоммуникаций, Управление качеством и вероятностные модели функционирования сетей связи следующего поколения, Мультисервисные сети связи, научно-исследовательская работа.

Требования к результатам освоения дисциплины:

Процесс изучения дисциплины «Современные концепции управления инфокоммуникациями» направлен на формирование следующих компетенций:

ОК: 3, 7; ПК: 4-8, 14, 15, 20, 21, 24

(указываются в соответствии с ФГОС ВПО)

- способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности (ОК- 3);

- способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности (ОК- 7);
- способность демонстрировать знания фундаментальных и смежных прикладных разделов специальных дисциплин магистерской программы, знания общеметодологического характера, знания истории развития информатики и информационных технологий (ПК-4);
- способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математике, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий, а также знания, которые находятся на передовом рубеже данной науки (ПК-5);
- способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять своё научное мировоззрение (ПК-6);
- способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности (ПК-7);
- способность разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач проектной и производственно-технологической деятельности (ПК-8);
- способность разрабатывать корпоративную техническую политику развития корпоративной инфраструктуры информационных технологий на принципах открытых систем (ПК-14);
- способность разрабатывать корпоративные стандарты и профили функциональной стандартизации приложений, систем, информационной инфраструктуры (ПК-15);
- способность разрабатывать аналитические обзоры состояния области информационных технологий по направлениям профильной подготовки (ПК-20);
- способность выполнять работу экспертов в ведомственных, отраслевых или государственных экспертных группах по экспертизе проектов, тематика которых соответствует профилю подготовки магистра информационных технологий (ПК-21);
- способность участвовать в деятельности профессиональных сетевых сообществ по конкретным направлениям (ПК-24).

В результате изучения дисциплины «Современные концепции управления инфокоммуникациями» студент должен:

Знать:

- базовые понятия систем и сетей инфокоммуникаций;
- общие характеристики концепций, архитектур, стандартов современных систем и сетей инфокоммуникаций;

– основные принципы управления современными системами и сетями инфокоммуникаций
– современные концепции управления инфокоммуникациями в области концепций, архитектур, моделей и методов управления инфокоммуникациями

Уметь:

– осуществлять анализ принципов построения архитектур сетей IP и мультисервисных сетей следующего поколения
– анализировать принципы построения, архитектур и методологий систем управления инфокоммуникациями.

Владеть*:* навыками и подходами в области анализа и построения архитектур, моделей и методов управления инфокоммуникациями.

Содержание дисциплины

Содержание разделов дисциплины

1. **Базовая часть**
   (a) Модель ISO/OSI.
   (b) Стеки протоколов (TCP/IP, IEEE 802, SS7, H.323 и др.).
   (c) Физический уровень, кодирование сигнала, мультиплексирование (TDM, FDM, OFDM).
   (d) Канальный уровень, множественный доступ (TDMA, FDMA, CDMA, OFDMA).
   (e) Сетевой и транспортный уровни (IP, IPv6, MPLS, TCP, UDP, SCTP, RTP) стека TCP/IP.
   (f) Конвергентные сети
      i. Интеллектуальные сети (ИСС)
      ii. Softswitch
      iii. H.323
      iv. IMS, SIP, SIGTRAN(+SS7)
2. **Сети 2G.**
   (a) GSM.
   (b) GPRS, EDGE
   (c) CDMA, D-AMPS
3. **Сети 3G.**
   (a) UMTS.
   (b) CDMA2000
4. **Сети 4G.**
   (a) WiMAX.
   (b) LTE.

Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература

1. Таненбаум Э. Компьютерные сети (3 или 4 изд.) // Спб.: Изд-во «Питер», 2007. – 992 с.
2. Самуйлов К.Е. Методы анализа и расчета сетей ОКС7 // М. Изд-во РУДН, 2002
3. Кулябов Д.С., Королькова А.В. Архитектура и принципы построения современных сетей и систем телекоммуникаций Уч. пособие // Москва, Изд-во РУДН, 2008
4. В. Вишневский, С. Портной, И. Шахнович Энциклопедия WiMAX. Путь к 4G, 2010
5. Х. Кааранен, А. Ахтиайнен, Л. Лаитинен, Сети UMTS. Архитектура, мобильность, сервисы, 2007
6. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH. — СПб.: БХВ. — Санкт-Петербург, 2006. — 368 с.
7. Гольдштейн Б.С. Интеллектуальные сети. Издательство: Радио и связь, 2000.

б) дополнительная литература

1. Гольдштейн Б.С. Телекоммуникационные протоколы. Протоколы стека ОКС7: подсистема МАР. Кн. 10,2012
2. Jesse Russell W-CDMA (UMTS), 2012
3. Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский Сети связи, 2011
4. Gottfried Punz Evolution of 3G Networks: The Concept, Architecture and Realization of Mobile Networks Beyond UMTS, 2010
5. Б. С. Гольдштейн, А. А. Зарубин, В. В. Саморезов Протокол SIP. Справочник, 2005
6. Наумов В.А., Самуйлов К.Е., Яркина Н.В. Теория телетрафика мультисервисных сетей. - М.: Изд-во РУДН, 2007. - 191 с.
7. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. — М.: Издательский дом ”Вильямс”, 2004. — 304 с.
8. Вишневский В., Ляхов А., Портной С, Шахнович И. Широкополосные беспроводные сети передачи информации. — М.: Эко-Трендз, 2005. — 592 с.
9. Гулевич Д. С. Сети связи следующего поколения. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий. ИНТУИТ.ру, 2007.

в) программное обеспечениеОС Linux, VirtualBox, Asterix, ekiga

г) базы данных, информационно-справочные и поисковые системы: не предусмотрено

Материально-техническое обеспечение дисциплины:

Занятия проводятся на базе лаборатории «Управление инфокоммуникациями» кафедры систем телекоммуникаций РУДН, созданной для выполнения

Инновационной образовательной программы в рамках в рамках национального проекта «Образование» правительства Российской Федерации. Лаборатория состоит из трех подразделений - учебного (ауд. 110), учебно-научного (ауд.116) и научного (ауд. 123), и оснащена современным сетевым оборудованием и компьютерной техникой. Лабораторная база позволяет осуществлять проекты по разработке прикладных средств инфокоммуникационной среды, проводить лекционные и лабораторные занятия с мультимедийными средствами обучения.

Методические рекомендации по организации изучения дисциплины:

На освоение дисциплины отводится один семестр. В качестве итогового контроля знаний предусмотрен зачёт. Для текущего контроля успеваемости и промежуточной аттестации студентов рекомендуется использовать вопросы и задания подобные перечисленным ниже.

Примерный перечень вопросов контрольной работы

1. Технология MPLS.
2. Уровневое построение сети NGN.
3. Протоколы сигнализации в сетях с коммутацией пакетов.
4. Управление инфокоммуникациями по концепции TMN.
5. Уровневое представление сети телекоммуникаций – управление, сигнализация, соединения, транспорт.

Список вопросов

1. Технология MPLS.
2. Уровневое построение сети NGN.
3. Протоколы сигнализации в сетях с коммутацией пакетов.
4. Управление инфокоммуникациями по концепции TMN.
5. Уровневое представление сети телекоммуникаций – управление, сигнализация, соединения, транспорт.
6. Общий обзор технологий канального уровня для построения локальных сетей.
7. Общий обзор технологий построения глобальных и городских сетей.
8. Технология Ethernet как наиболее распространенная технология построения сетей.
9. Протокол IP как основной протокол интернет. Адресация IPv4.
10. Протокол IPv6 как эволюционное развитие протокола IPv4.
11. Недостатки протокола TCP, его сравнение с протоколом SCTP.
12. Протокол DNS. Разрешение адресов IPv4, IPv6, сервисные записи DNS, адресация ENUM.
13. Обеспечение качества обслуживания в IP-сетях.

14. MPLS: история развития, связь с ATM. Сравнение сферы применения MPLS и классической маршрутизации.
15. Общая концепция NGN. Протокол SIP.
16. Сравнение идеологий Softswitch и IMS.
17. Основные протоколы стека H.323.
18. Схема взаимодействия по протоколу H.323.
19. Схема взаимодействия по протоколу SIP.
20. Возможные схемы взаимодействия IP-сетей и ТфОП.

Фонды оценочных средств

Словарь (глоссарий) основных терминов и понятий

Asynchronous Transfer Mode (ATM) — мультисервисная, высокоскоростная технология асинхронной переда чи данных (ячеек небольшого размера фиксированной длины — по 53 байта) со встроенной поддержкой обеспечения гарантированного каче ства обслуживания (QoS); может применяться при построении маги стральных сетей, например, поверх SONET/SDH.

Bluetooth — технология, обеспечивающая беспроводную передачу данных на небольшие расстояниях между различными устройствами (например, мобильными персональными компьютерами, мобильными телефонами и другими устройствами) в режиме реального времени.

Edge LSR (E-LSR) — маршрутизатор на границе сети MPLS, осуществляющий классификацию поступающих в MPLS-сеть пакетов, их фильтрацию, управление трафиком и т.п.

ENUM — сетевой протокол, определяющий выбор маршрутов для связи с различными устройствами, принадлежащими одному абоненту (пользователю телефонного номера в международном формате E.164), и устанавливающий соответствие между номером в формате E.164 (международный формат телефонных номеров, определяемый в Рекомендации E.164 ITU) и доменным именем (Domain Name System, DNS).

Frame Relay (FR) — технология доставки сообщений в сетях передачи данных с коммутацией пакетов; может использоваться для управления пульсирующим трафиком между локальными сетями и территориальной сетью, а также для передачи голоса, причём для передачи служебной информации используется специально выделенный канал сигнализации.

IMS (IP Multimedia Subsystem) — концепция, определяющая сетевую архитектуру, которая опирается на пакетную транспортную сеть и обеспечивает управление сеансами связи и доставку в рамках этих сеансов любых типов информации — речи, данных, видео, мультимедиа.

Label-Switch Router (LSR) — маршрутизатор сети MPLS, поддерживающий как обычную маршрутизацию IP, так и коммутацию по меткам.

MPLS — механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов.

Softswitch — носитель интеллектуальных возможностей сети, который координирует управление обслуживанием вызовов, сигнализацию и функции, обеспечивающие установление соединения через одну или несколько сетей.

WiMax (Worldwide Interoperability for Microwave Access) — стандарт беспроводной связи IEEE 802.16.

Архитектура сети — набор уровней и протоколов.

Звено сигнализации SS7 (Signaling Link, SL) — канал передачи данных, соединяющий между собой пункты сигнализации и состоящий из физического канала связи, терминального сигнального оборудования и протокола, контролирующего соединение.

Инфокоммуникационная услуга / приложение – возможность удовлетворить потребность человека в автоматизированной обработке, хранении или предоставлении по запросу информации различного рода с использованием средств вычислительной техники как на входящем, так и на исходящем конце соединения. Примерами услуги/приложения могут служить электронная почта (e-mail), приложение для удаленного доступа типа Telnet, услуга конференции в реальном времени (веб-чат, мгновенный обмен сообщениями), услуга индивидуального просмотра видеофильма по запросу (video-on-demand) и др.

Коммутация каналов — режим передачи, при котором формируется составной канал (соединение) через несколько транзитных узлов из нескольких последовательно «соединённых» каналов на время передачи информации (до разъединения соединения).

Коммутация пакетов — режим передачи сообщений, при котором сообщения разбиваются на пакеты ограниченного размера, причём канал передачи занят только во время передачи пакета и освобождается после её завершения.

Коммутация сообщений — режим передачи, включающий приём, хранение, выбор исходящего направления и дальнейшую передачу сообщений без нарушения их целостности.

Мультисервисная сеть — инфраструктура, использующая единый канал для передачи данных разных типов трафика.

Протокол (сетевой протокол) — набор правил, позволяющий осуществлять соединение и обмен данными между двумя включёнными в сеть компьютерами; набор правил, описывающих формат и назначение пакетов, которыми обмениваются одноранговые сущности.

Пункт сигнализации SS7 (Signaling Point, SP) — любой узел сигнальной сети, реализующий функции обработки сигнальных сообщений SS7.

Сервис или услуга (Service) — набор примитивов, которые предоставляются вышележащему уровню нижележащим; описывает интерфейс между двумя уровнями, в котором нижележащий уровень является поставщиком услуги, а вышележащий — её потребителем.

Сеть связи — Совокупность линий связи и промежуточного оборудования/ промежуточных узлов, терминалов/оконечных узлов, предназначенных

для передачи информации от отправителя до получателя с заданными параметрами качества обслуживания.

Сеть связи следующего поколения (Next Generation Network, NGN) — концепция построения сетей связи, обеспечивающих предоставление неограниченного набора услуг за счёт унификации сетевых решений, предполагающая реализацию универсальной транспортной сети с распределённой коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи

Система общеканальной сигнализации No7 — обеспечивает связь между коммутационными станциями и специализированными узлами сетей связи.

Стек протоколов — используемый системой список протоколов.

Традиционная сеть связи – специализированная сеть связи, такая как телефонная сеть общего пользования (ТфОП), сеть передачи данных общего пользования (СДОП), сеть кабельного телевидения и т. п., изначально предназначенная для предоставления услуг связи одного вида.

Транзитный пункт сигнализации SS7 (Signaling Transfer Point, STP) — пункт сигнализации, осуществляющий только функции маршрутизации сигнальных сообщений между различными звеньями сигнализации и не имеющий подсистем пользователей.

Хэндовер – процедура смены радиоканала без разрыва текущего соединения благодаря

Цифровая сеть с интеграцией служб (ISDN) — сеть с коммутацией каналов (телефонная сеть), обеспечивающая полностью цифровые соединения между оконечными устройствами для поддержания широкого спектра информационных услуг.

Шлюз (Gateway) — сетевое устройство, соединяющее отдельные сегменты сети с разными типами системного и прикладного программного обеспечения.

Методические указания для преподавателя, студента, слушателя

На освоение дисциплины отводится 1 семестр. В качестве итогового контроля знаний предусмотрены экзамены. Упражнения, лекции, методику, тестирования и задания для самостоятельной работы студентов можно увидеть в разделе «Фонды оценочных средств» данного учебно-методического комплекса.

Лабораторный практикум по дисциплине

Лабораторная работа № 1
Установка Asterisk на виртуальную машину.
Лабораторная работа № 2
Настройка SIP-телефона.

Перечень рефератов и/или курсовых работ по темам

1. Стандарт Long Term Evolution (LTE) — от 2G к 4G.
2. В реферате следует описать эволюцию и современное состояние сетей связи, подробно остановиться на , привести примеры реализованных коммерческих сетей LTE.
3. Основные протоколы сетей связи следующего поколения. В реферате необходимо перечислить и охарактеризовать основные протоколы передачи информации, применяемые в сетях связи следующего поколения - H.323, SIP, MGCP, MEGACO/H.248, BICC, Sigtran.
4. Технология Sigtran передачи сигнального трафика по IP-сетям. В реферате следует описать архитектуру и функциональные элементы Sigtran, а также протоколы стека Sigtran, остановиться на месте протокола SCTP в стеке протоков Sigtran, изложить основные принципы передачи информации по протоколу SCTP, отличия от протокола TCP.
5. Протокол инициирования сеансов связи Session Initiation Protocol (SIP). В реферате необходимо изложить основные принципы протокола SIP, описать способы интеграции протокола SIP с IP-сетями, принципы адресации в SIP-сетях. Следует описать архитектуру сети на базе протокола SIP, основные функциональные элементы SIP-сети, указать типовые сценарии установления сеанса связи по протоколу SIP. Необходимо описать структуру сообщений протокола SIP, типы запросов для протокола SIP, предложить подход к анализу влияния протокола SIP на показатели качества в сетях NGN.
6. Алгоритм Кауфмана-Робертса для модели MCC.
7. Технология peer-to-peer (P2P): принципы, примеры использования. Сети P2P.
8. Протокол IGMP (Internet Group Management Protocol)
9. Междоменный протокол BGMP (Boarder Gateway Multicast Protocol)
10. Алгоритмы RPB (Reverse Path Broadcasting) и TRPB (Truncated Reverse Path Broadcasting), алгоритм RPM (Reverse Path Multicasting)
11. Алгоритм и протокол CBT (Core-Based Tree)
12. Протокол DVMRP (Distance-Vector Multicast Routing Protocol)
13. Протокол MOSPF (Multicast Open Shortest Path First)
14. Протокол PIM-DM (Protocol Independent Multicast - Dense Mode)
15. Протокол PIM-SM (Protocol Independent Multicast – Sparse Mode)
16. Мультивещание в сетях подвижной связи: протоколы MoM (Mobile Multicast) и MMA (Multicast by Multicast Agent)

Тестовые задания по темам (для текущего и промежуточного самоконтроля)

Примерные тестовые задания по дисциплине представлены ниже.

1. Дерево доставки отличается от дерева кратчайших путей тем, что оно:
   (a) Не всегда определяет кратчайший путь доставки

(b) Доступно только узлам, запрашивающим пакеты
(c) Строится динамически
(d) Обеспечивает эффективную доставку

2. Лавинный алгоритм (Flooding) не позволяет:
(a) Построить дерево доставки
(b) Осуществлять доставку группового трафика
(c) Обеспечивать доставку дейтаграмм между соседними маршрутизаторами
(d) Устранять проблему дублирования дейтаграмм
3. Основным достоинством алгоритма RPB заключается в том, что:
(a) Он требует, чтобы маршрутизаторы владели информацией обо всем остовом дереве
(b) Он не подразумевает специальных механизмов остановки процесса передачи
(c) Он создает дерево доставки частично
(d) Он может работать без протокола IGMP
4. Какой из следующих алгоритмов является самым эффективным для групповой доставки?
(a) RPM
(b) RPB
(c) TRPB
(d) Spanning Tree
5. В алгоритме CBT сообщение от маршрутизатора в направлении ядра для первоначального соединения называется:
(a) JOIN_ACK
(b) JOIN_REQUEST
(c) ECHO_REQUEST
(d) ECHO_REPLY
6. В алгоритме формирования дерева на основе ядра (CBT) родительским называется интерфейс по направлению:
(a) От ядра к члену группы
(b) От маршрутизатора к члену группы
(c) От члена группы к ядру
(d) От члена группы к узловому маршрутизатору
7. Что является самым большим недостатком протокола DVMRP?
(a) Недостаточная масштабируемость
(b) Порождение регулярных всплесков служебного трафика
(c) Генерация небольшого объема служебной информации
(d) Неполное соответствие стандартным нормам
8. Какое из следующих утверждений неверно?
(a) Сообщения IGMP передаются в IP дейтаграммах
(b) Хост отправляет первый IGMP отчет, когда первый процесс вступает в группу
(c) IGMP имеет сообщение фиксированного размера
(d) В качестве ”ведущего” выбирается маршрутизатор с наибольшим IP-адресом

9. По умолчанию значение 1 для TTL групповых дейтаграмм позволяет дейтаграмму распространяться:
   (a) Только в своей подсети
   (b) Только по всей сети
   (c) По распределенной сети
   (d) Между соседними маршрутизаторами
10. Какой из следующих элементов не входит в модель IP-мультивещания поверх ATM - RFC 2022 ?
   (a) Сервер разрешения адресов мультивещания (MARS)
   (b) Клиенты сервера MARS
   (c) Сервер мультивещания(MSC)
   (d) Абстрактный групповой ATM-адрес
11. Технология LANE не обеспечивает:
   (a) Пакетирование и передачу данных
   (b) Распознавание адресов
   (c) Управление групповой рассылкой сообщений
   (d) Выбор лучшей таблицы маршрутизации при любой передачи
12. Метод двунаправленного туннелирования используется:
   (a) При удаленной подписке
   (b) В алгоритме CBT
   (c) В протоколе MoM
   (d) В сетях с неподвижными узлами
13. Основным отличием протокола MMA от MoM является использование:
   (a) Агентов
   (b) Перенаправителей
   (c) Метода туннелирования
   (d) Дерева доставки
14. Протокол IGMP используется для:
   (a) Управления группой
   (b) Одноадресной передаче данных
   (c) Управления маршрутизацией
   (d) Построения дерева доставки
15. Протокол TRPB предложен вместо RPB, чтобы решить проблему:
   (a) Вычисления самого короткого пути
   (b) Определения отправителя сообщения
   (c) Порождения ненужного трафика в подсети, не содержащей получателей
   (d) Определения получателя сообщения
16. Протоколы IGMP, DVMRP, MOSPF, PIM:
   (a) Взаимозаменяемы
   (b) Являются протоколами управления группой
   (c) Являются протоколами многоадресной маршрутизации
   (d) Работают с протоколом передачи данных IP
17. Сколько основных видов PIM (Protocol Independent Multicast) имеется?
   (a) 1 (один)
   (b) 2 (два)
   (c) 3 (три)

(d) 4 (четыре)

18. Какой из следующих принципов неприменим к классификации протоколов групповой маршрутизации?
    (a) Требуемый протокол класса IGP (EGP)
    (b) Алгоритм построения деревьев доставки
    (c) Применение на прикладном уровне
    (d) Оптимальные условия доставки
19. Сколько RP алгоритмов (по обратному пути) применяются в данный момент?
    (a) 1(один)
    (b) 2(два)
    (c) 3(три)
    (d) 4(четыре)
20. Какое из следующих понятий нехарактерно для протокола BGMP?
    (a) Домен
    (b) Корневой домен
    (c) Информационная база маршрутизации
    (d) Точка встречи (Rendezvous Point)

Тренинговые задания

В качестве тренинговых заданий рекомендуется использовать все упражнения лабораторного практикума.

Перечень вопросов итоговой аттестации по курсу

1. Технология MPLS.
2. Уровневое построение сети NGN.
3. Протоколы сигнализации в сетях с коммутацией пакетов.
4. Управление инфокоммуникациями по концепции TMN.
5. Уровневое представление сети телекоммуникаций – управление, сигнализация, соединения, транспорт.

**К. Е. Самуйлов, Д. С. Кулябов, А. В. Королькова,
Ю. В. Гайдамака, И. А. Гудкова, П. О. Абаев**

Архитектура и принципы построения сетей связи следующих поколений

Учебное пособие

Часть I

Базовая часть

Глава 1. Общая характеристика проблемной области. Базовые понятия в области систем и сетей. телекоммуникаций. Стандартизирующие организации

1.1. Базовые понятия в области систем и сетей телекоммуникаций

1.1.1. Сеть связи. Режимы передачи. Технологии коммутации

Сеть связи — это совокупность линий связи и промежуточного оборудования/промежуточных узлов, терминалов/оконечных узлов, предназначенных для передачи информации от отправителя до получателя с заданными параметрами качества обслуживания.

Линия связи представляет собой совокупность физической среды распространения сигналов и оборудования, формирующих специализированные каналы, имеющие определённые стандартные показатели: полосу частот, скорость передачи и т.п.

Каналы связи могут быть *непрерывными (аналоговыми)* и *дискретными (цифровыми)*. Также каналы связи различаются по направленности передачи. Выделяют три типа передачи информации:

- *симплексная передача (Simplex Transmission)* — передача данных в одном, предварительно определённом направлении;
- *полудуплексная передача (Half-Duplex Transmission)* — передача данных, при которой данные пересылаются в обоих направлениях, но только в одном направлении в каждый момент времени;
- *дуплексная передача (Duplex Transmission)* — передача данных, при которой данные пересылаются одновременно в обоих направлениях.

Обмен информацией между узлами сети обеспечивается с помощью *технологий коммутации*:

- *коммутация каналов (Circuit Switching)* — режим передачи, при котором формируется составной канал (соединение) через несколько транзитных узлов из нескольких последовательно «соединённых» каналов на время передачи информации (до разъединения соединения);
- *коммутация сообщений (Messege Switching)* — режим передачи, включающий приём, хранение, выбор исходящего направления и дальнейшую передачу сообщений без нарушения их целостности;
- *коммутация пакетов (Packet Switching)* — режим передачи сообщений, при котором сообщения разбиваются на пакеты ограниченного размера, причём канал передачи занят только во время передачи пакета и освобождается после её завершения;

– *коммутация ячеек (Cell Switching)* — режим передачи пакетов фиксированного размера.

1.1.2. Понятие протокола. Иерархия протоколов. Интерфейсы и сервисы

В широком смысле под протоколом понимается правило взаимодействия двух сущностей. Сетевой протокол определяет набор правил, позволяющих осуществлять соединение и обмен информацией между двумя элементами (узлами) сети.

Большинство протоколов строится как иерархический набор *уровней (Layers)*, каждый последующий из которых вводится над предыдущим (рис. 1.1). Нижележащий уровень предоставляет некоторый набор услуг (сервисов) для вышележащего, скрывая детали реализации предоставляемой услуги.

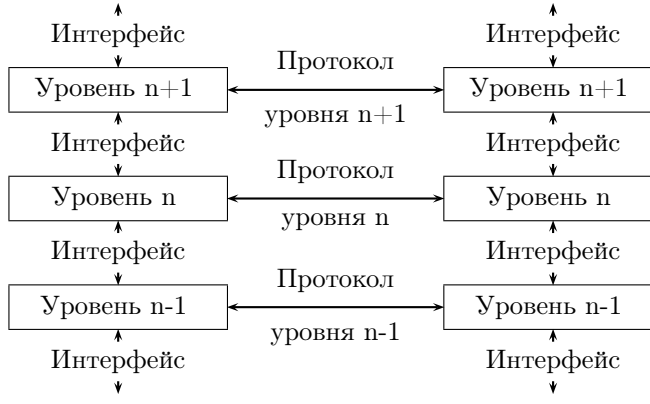

Рис. 1.1. Уровни протоколов

Взаимодействие производится между уровнем n одного узла и уровнем n другого. Используемые правила и соглашения называются *протоколом уровня* n. Между парой смежных уровней находится *интерфейс*, определяющий набор сервисов, предоставляемых нижележащим уровнем вышележащему.

Активный элемент каждого уровня называется *сущностью (Entity)*. Сущности одного уровня на разных узлах называются *одноранговыми сущностями*. Сущности уровня n (*поставщики услуг*) реализуют услуги, используемые уровнем $n+1$ (*потребители услуг*). Для предоставления этих услуг уровень n может использовать услуги уровня $n-1$.

Сервис, или услуга (Service), представляет собой набор примитивов, которые предоставляются вышележащему уровню нижележащим. Сервис определяет, какие именно операции уровень будет выполнять от лица своих пользователей, но никак не оговаривает, как должны реализовываться эти операции. Сервис описывает интерфейс между двумя уровнями, в котором нижележащий уровень является поставщиком услуги, а вышележащий — её потребителем.

Протокол определяет набор правил, описывающих формат и назначение пакетов, которыми обмениваются одноранговые сущности внутри уровня. Сущности используют протокол для реализации определений их сервисов. Протоколы могут меняться, но предоставляемые услуги должны оставаться неизменными.

Услуги доступны через *точки доступа к услуге (Service Access Point, SAP)*. Чтобы два уровня могли обмениваться информацией, необходима договорённость о наборе правил используемого интерфейса. Сущность уровня $n+1$ передаёт *элемент данных интерфейса (Interface Data Unit, IDU)*, состоящий из *элемента данных услуги (Service Data Unit, SDU)* и некоторой *управляющей информации (Interface Control Information, ICI)*, сущности с номером n через точку SAP. Для передачи SDU сущности уровня n может понадобиться разбить его на несколько фрагментов и послать их в виде отдельных *элементов данных протокола (Protocol Data Unit, PDU)* или *пакетов*.

По типу установления соединения протоколы можно разделить на два типа:

- протоколы с *установлением соединения (Connection Oriented)* — перед обменом данными отправитель и получатель должны сначала установить соединение и, возможно, выбрать некоторые параметры протокола, а после завершения сеанса они должны разорвать соединение;
- протоколы *без предварительного установления соединения (Connectionless)*, или *датаграммные (дейтаграммные)* протоколы — передача данных осуществляется, не дожидаясь установления соединения.

Используемый системой список протоколов называется *стеком протоколов*. Набор уровней и протоколов называется *архитектурой сети*.

1.2. Принципы классификации сетей телекоммуникаций

Сети телекоммуникаций можно классифицировать[1] по нескольким параметрам:

1. по размеру сети:
   - *локальные сети (Local Area Network, LAN)* — сети здания или организации;
   - *региональные сети (Metropolitan Area Network, MAN)* — сети уровня города или региона;

[1] Заметим, что мы строим классификацию, а не таксономию.

- *глобальные сети (Wide Area Network, WAN)* — сети, охватывающие большие территории и включающие в себя десятки и сотни тысяч компьютеров;

2. по типу коммутации:
   - сети с коммутацией пакетов (например, TCP/IP, IPX/SPX, ATM, сети сотовой связи 3G);
   - сети с коммутацией каналов (например, ТфОП, сети сотовой связи 1G и 2G);
   - смешанные (например, сети сотовой связи 2,5G);
3. по установлению виртуального канала:
   - с установлением виртуального канала (например, сети X.25, Frame Relay, ATM, ТфОП);
   - без установления виртуального канала (например, TCP/IP, IPX/SPX);
4. по используемому стеку протоколов;
5. по количеству используемых стеков протоколов:
   - монопротокольные сети;
   - мультипротокольные сети (например, IP over ATM, IP over SDH/SONET);
6. по спектру оказываемых услуг:
   - моносервисные сети (передача данных, передача голоса);
   - мультисервисные сети;
7. по типу передаваемой информации:
   - сети передачи данных;
   - сети передачи голоса;
   - сети передачи видео;
8. по наличию сигнализации:
   - сети с выделенной сигнализацией (SS7);
   - сети без выделенной сигнализации (TCP/IP);
9. по топологии сети:
   - сети с топологией шина;
   - сети с топологией кольцо;
   - сети с топологией звезда;
   - сети со смешанной топологией;
10. по среде передачи:
    - проводные сети:
      - связь осуществляется по медному кабелю;
      - связь осуществляется по оптоволокну;
    - беспроводные сети.

1.3. Стандартизирующие организации

Организации в международной системе стандартизации можно разделить следующим образом:

- официальные международные организации стандартизации:

- *Международная организация по стандартизации (International Organization for Standardization, ISO)*
  Создана в 1946 г., включает в себя национальные организации стандартизации из 157 стран мира, в частности, ANSI (США), Федеральное агентство по техническому регулированию и метрологии (Россия), BSI (Великобритания), AFNOR (Франция) и др., обладает полномочиями для координирования на международном уровне разработки различных промышленных стандартов и принятия их в качестве международных стандартов.
- *Международный союз электросвязи, МСЭ (International Telecommunication Union, ITU[1])*
  Занимается стандартизацией международных средств связи и состоит из трёх основных секторов:
  - сектор стандартизации телекоммуникаций (ITU-T[2]) — занимается вопросами, связанными с телефонными системами и системами передачи данных[3];
  - сектор радиосвязи (ITU-R) — распределяет радиочастоты между конкурирующими компаниями, решает спорные вопросы в данной области;
  - сектор развития (ITU-D) — занимается вопросами стратегии и политики развития систем электросвязи;

- региональные организации стандартизации:
  - *Европейский институт стандартизации в области телекоммуникаций (European Telecommunications Standards Institute, ETSI)*
    Создан в 1988 г. Отвечает за стандартизацию информационных и телекоммуникационных технологий в пределах Европы.
  - *Центр сетевых информационных технологий АзиатскоТихоокеанского региона (Asia Pacific Network Information Centre, APNIC)*
    Отвечает за распределение сетевых ресурсов в Азиатскотихоокеанском регионе;
- национальные организации стандартизации:
  - *Федеральное агентство по техническому регулированию и метрологии (Россия)*;
  - *Американский институт национальных стандартов (American National Standards Institute, ANSI)*;
  - и др.;
- промышленные консорциумы:
  - *Сообщество инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE)*

---

[1] *ITU также принято переводить как Международный телекоммуникационный союз.*

[2] С 1956 по 1993 г. ITU-T именовался CCITT (Comité Consultatif International Télégraphique et Téléphonique) — Консультативный комитет по международной телефонной и телеграфной связи.

[3] Рекомендации ITU-T часто становятся международными стандартами, хотя правительство любой страны может принять или проигнорировать их.

Целью данной организации является продвижение теоретических и прикладных достижений электротехнической и электронной индустрии.

– *Рабочая группа по проектированию Интернет-технологий (Internet Engineering Task Force, IETF)*
IETF представляет собой сообщество разработчиков, операторов, изготовителей и исследователей в области сетевых технологий. В основе Интернетстандартизации лежит технология издания и поддержания RFCдокументов — спецификаций, разработанных различными организациями и рабочими группами IETF.
– *Интернет-сообщество (Internet Society, ISOC)*
ISOC представляет собой ассоциацию экспертов, отвечающих за разработку стандартов технологий сети Интернет.
– *Консорциум, специализирующийся в области разработки и развития стандартов WWW-технологий (World Wide Web Consortium, W3C).*

Глава 2. Модель ISO/OSI. Иерархия протоколов различных стеков относительно модели ISO/OSI

2.1. Обзор эталонной модели OSI

В начале 1980-х гг. ряд международных организаций по стандартизации (ISO, ITU-T) разработали *эталонную модель взаимодействия открытых систем (International Standards Organization / Open System Interconnection Reference Model, ISO/OSI)*. Модель ISO/OSI чётко определяет уровни взаимодействия систем, стандартизует имена уровней и указывает услуги и функции каждого уровня (рис. 2.1).

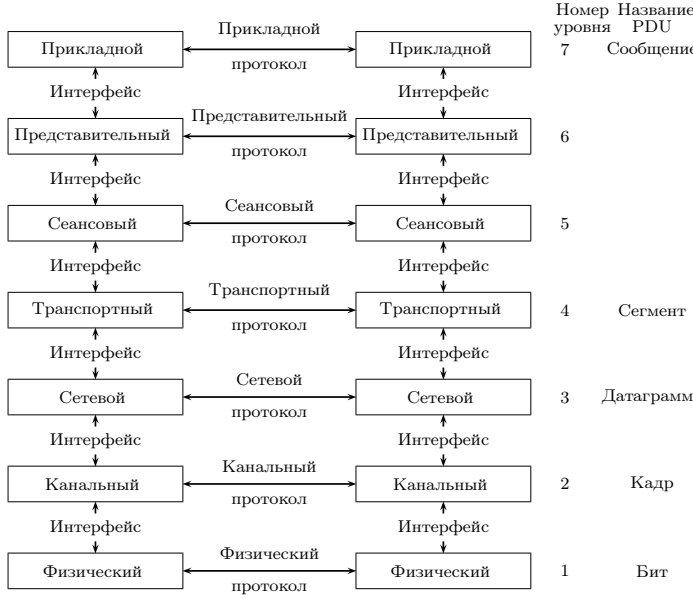

Рис. 2.1. Эталонная модель ISO/OSI

2.1.1. Принципы построения эталонной модели ISO/OSI

Эталонная модель ISO/OSI базируется на следующих принципах:

1. уровень должен создаваться по мере необходимости выделения отдельного уровня абстракции;
2. каждый уровень должен выполнять строго определённую функцию;
3. функции для каждого уровня должны выбираться с учётом создания стандартизованных международных протоколов;
4. границы между уровнями должны выбираться так, чтобы поток данных между интерфейсами был минимальным;
5. количество уровней должно быть достаточно большим, чтобы различные функции не объединялись в одном уровне без необходимости, но не слишком высоким, чтобы архитектура не становилась громоздкой.

2.1.2. Уровни в модели OSI

Одним из важнейших принципов OSI является то, что сетевые системы взаимодействуют друг с другом на одинаковых уровнях модели. Дадим краткое описание уровней модели OSI (рис. 2.1).

2.1.2.1. Уровень 1: Физический уровень

Физический уровень (Physical Layer) обеспечивает передачу битовых потоков без каких-либо изменений между логическими объектами уровня звена данных по физическим соединениям.

На данном уровне определяются базовые механизмы кодирования и декодирования двоичных данных в физическом носителе, а также специфицируются соединители, но не сама среда. Среда, согласно эталонной модели, рассматривается как нечто, лежащее ниже физического уровня. Битовый поток в носителе должен быть независим от типа среды.

Физический уровень предоставляет канальному уровню следующие услуги и элементы услуг:

- физические соединения;
- физические сервисные блоки данных;
- физические оконечные пункты соединения;
- осуществляет идентификацию канала данных;
- осуществляет упорядочение;
- осуществляет оповещение об ошибках;
- определяет параметры качества услуги.

На физическом уровне выполняются следующие функции:

- активизация и деактивизация физического соединения;
- передача физических сервисных блоков данных;
- административное управление физическим уровнем.

2.1.2.2. Уровень 2: Канальный уровень

Канальный уровень (Data Link Layer) также носит названия *уровень управления передачей данных (Data Link Control, DLC)* или *уровень звена данных*.

Канальный уровень обеспечивает функциональные и процедурные средства для установления, поддержания и разрыва соединений канального уровня между сетевыми логическими объектами и для передачи сервисных блоков данных этого уровня. Соединение канального уровня строится на основе одного или нескольких физических соединений.

Канальный уровень обнаруживает и по возможности исправляет ошибки, которые могут возникнуть на физическом уровне. Кроме того, канальный уровень обеспечивает для сетевого уровня возможность управлять подключением каналов данных на физическом уровне. Единицу информации на канальном уровне называют *кадром (Frame)*.

Канальный уровень предоставляет следующие услуги или элементы услуг сетевому уровню:

- соединение канального уровня;
- сервисные блоки данных канального уровня;
- идентификаторы оконечного пункта соединения канального уровня;
- осуществляет упорядочение блоков данных;
- осуществляет оповещение об ошибках;
- управляет потоком данных;
- определяет параметры качества услуги.

На канальном уровне выполняются следующие функции:

- установление и разрыв соединения канального уровня;
- отображение сервисных блоков данных канального уровня;
- расщепление соединения канального уровня;
- разграничение и синхронизация;
- упорядочение блоков данных;
- обнаружение ошибок;
- восстановление при ошибках;
- управление потоком данных;
- идентификация и обмен параметрами;
- управление переключением каналов данных;
- административное управление канальным уровнем.

2.1.2.3. Уровень 3: Сетевой уровень

Сетевой уровень (Network Layer) предоставляет средства установления, поддержания и разрыва сетевого соединения, а также функциональные и процедурные средства для обмена по сетевому соединению сетевыми сервисными блоками данных между транспортными логическими объектами.

Сетевой уровень обеспечивает транспортным логическим объектам независимость от функций маршрутизации и ретрансляции, связанных с процессами установления и функционирования данного сетевого соединения.

Все функции ретрансляции и расширенные протоколы последовательного переноса данных, которые предназначены для поддержания сетевых услуг между оконечными открытыми системами, функционируют ниже транспортного уровня. Единицу информации на сетевом уровне называют *датаграммой или дейтаграммой (Datagram)*.

Основной услугой сетевого уровня является обеспечение передачи данных без каких-либо изменений между транспортными логическими объектами, т.е. структура и содержание данных, предоставляемых для передачи, определяется уровнями, расположенными выше сетевого.

Услуги, предоставляемые на каждом из концов сетевого соединения, одинаковы и в том случае, когда сетевое соединение проходит через несколько подсетей, каждая из которых предоставляет различные услуги.

Сетевой уровень предоставляет следующие услуги:

- сетевые адреса;
- сетевые соединения;
- сетевые идентификаторы оконечных пунктов соединения;
- осуществляет передачу сетевых сервисных блоков данных;
- определяет параметры качества услуги;
- оповещает об ошибках;
- упорядочивает блоки данных;
- управляет потоком данных;
- осуществляет передачу срочных сетевых сервисных блоков данных;
- осуществляет сброс;
- осуществляет разрыв сетевого соединения.

Некоторые из этих услуг являются необязательными, т.е.:

- пользователь должен запросить услугу;
- поставщик сетевой услуги может удовлетворить запрос или сообщить, что запрошенная услуга недоступна.

Функции сетевого уровня обеспечивают использование различных конфигураций для поддержки сетевых соединений: от соединений, поддерживаемых двухпунктовыми сетевыми конфигурациями, до сетевых соединений, поддерживаемых сочетаниями подсетей с различными характеристиками.

Сетевой уровень выполняет следующие функции:

- маршрутизацию и ретрансляцию;
- организацию сетевых соединений;
- мультиплексирование сетевого соединения;
- сегментирование и объединение;
- обнаружение ошибок;
- восстановление при ошибках;
- упорядочение блоков данных;
- управление потоком данных;
- передачу срочных данных;
- сброс;
- выбор услуги;
- административное управление сетевым уровнем.

2.1.2.4. Уровень 4: Транспортный уровень

Транспортный уровень (Transport Layer) обеспечивает передачу данных без каких-либо изменений между сеансовыми логическими объектами и

освобождает их от выполнения операций, обеспечивающих надёжную и экономически эффективную передачу данных.

Транспортный уровень оптимизирует использование доступных сетевых услуг, чтобы обеспечить пропускную способность, требуемую каждым сеансовым логическим объектом, при минимальных затратах. Эта оптимизация достигается путём внесения ограничений, обусловленных совместными требованиями со стороны всех одновременно работающих сеансовых логических объектов, а также общим качеством и объёмом сетевых услуг, предоставляемых транспортному уровню.

Все протоколы, определённые на транспортном уровне, имеют межоконечный характер. Под окончаниями понимают связанные транспортные логические объекты. Поскольку сетевые услуги обеспечивают сетевые соединения между транспортными логическими объектами по принципу «каждый с каждым», включая использование последовательно соединённых подсетей, то транспортный уровень освобождается от функций маршрутизации и ретрансляции.

На транспортном уровне имеются функции, обеспечивающие требуемое качество услуг на основе услуг, предоставляемых сетевым уровнем. Качество сетевых услуг зависит от того, как они реализуются.

Транспортный уровень однозначно идентифицирует каждый сеансовый логический объект с помощью транспортного адреса. Транспортные услуги предоставляют средства для установления, поддержания и разрыва транспортного соединения. Транспортное соединение обеспечивает дуплексную передачу между двумя транспортными адресами.

Для одной пары транспортных адресов может быть установлено несколько транспортных соединений. Сеансовые логические объекты используют идентификаторы оконечных пунктов транспортных соединений, обеспечиваемые транспортным уровнем для распознавания этих пунктов.

Качество услуг при предоставлении транспортного соединения зависит от класса обслуживания, запрашиваемого сеансовым логическим объектом при установлении транспортного соединения. Выбранное качество обслуживания поддерживается в течение существования транспортного соединения.

Транспортным уровнем предоставляются следующие виды услуг:

- установление транспортного соединения;
- передача данных;
- разрыв транспортного соединения.

На транспортном уровне могут быть реализованы следующие функции:

- преобразование транспортного адреса в сетевой;
- межоконечное мультиплексирование транспортных соединений в сетевые;
- установление и разрыв транспортных соединений;
- межоконечное упорядочение блоков данных по отдельным соединениям;
- межоконечное обнаружение ошибок и необходимый контроль за качеством услуг;
- межоконечное восстановление после ошибок;
- межоконечное сегментирование, объединение и сцепление;
- межоконечное управление потоком данных по отдельным соединениям;

– супервизорные функции;
– передача срочных транспортных сервисных блоков данных.

2.1.2.5. Уровень 5: Сеансовый уровень

Сеансовый уровень (Session Layer) реализует службу имён (отображение логических имён в сетевые адреса), устанавливает сеансы между службами и создаёт точки для контрольной синхронизации в случае потери связи.

Сеансовый уровень выполняет следующие функции:
– отображение сеансового соединения на транспортное соединение;
– управление потоком данных в сеансовом соединении;
– передачу срочных данных;
– восстановление сеансового соединения;
– административное управление сеансовым уровнем.

2.1.2.6. Уровень 6: Уровень представления

Уровень представления (Presentational Layer) устанавливает способы представления информации, которой обмениваются прикладные логические объекты или на которую они ссылаются в процессе этого обмена.

Уровень представления охватывает два взаимодополняющих аспекта способов представления информации:
– представление данных, подлежащих передаче между прикладными логическими объектами;
– представление структуры данных, которую прикладные логические объекты намереваются использовать в своём диалоге, наряду с представлениями совокупности действий, которые могут быть выполнены над этой структурой данных.

На этом уровне определяется общий синтаксис (способы представления данных), но не семантика, которая известна только прикладным логическим объектам.

Уровень представления обеспечивает способы представления информации, которые являются общими для взаимодействующих прикладных логических объектов. Таким образом, прикладные логические объекты освобождаются от функции представления информации, поскольку используется общий способ представления, и для них обеспечивается синтаксическая независимость. Такая независимость может быть реализована двумя путями.

1. На уровне представления обеспечиваются элементы поддержки синтаксиса, являющиеся общими для использующих их прикладных логических объектов.
2. Прикладные логические объекты могут использовать произвольный синтаксис, а уровень представления обеспечивает преобразование этих синтаксисов. Для обмена между прикладными логическими объектами применяется общий синтаксис. Такое преобразование выполняется внутри открытой системы. На другие открытые системы это не влияет и, следова-

тельно, не оказывает влияние на стандартизацию протоколов уровня представления.

Уровень представления обеспечивает сеансовые услуги и добавляет к ним следующие возможности:

- преобразование синтаксиса;
- выбор синтаксиса.

Преобразование синтаксиса связано с преобразованием кодовых и символьных наборов, с модификацией расположения данных и с адаптацией действий над структурами данных. Выбор синтаксиса предоставляет средства первоначального выбора синтаксиса и последующего изменения сделанного выбора.

Прикладным логическим объектам предоставляются услуги сеансового уровня в виде услуг представления. На уровне представления выполняются следующие функции, с помощью которых реализуются услуги представления:

- запрос на установление сеанса;
- передача данных;
- соглашение по выбору и повторному выбору синтаксиса;
- преобразование синтаксиса, включая преобразование данных, форматирование и специальные функции преобразования;
- запрос на завершение сеанса.

2.1.2.7. Уровень 7: Прикладной уровень

Прикладной уровень (Application Layer) является наивысшим уровнем в эталонной модели OSI. Поэтому прикладной уровень не имеет интерфейса с более высоким уровнем. Он является единственным средством доступа прикладных процессов к функциональной среде OSI.

Прикладной уровень поддерживает локальные операционные системы, предоставляя им набор разнообразных протоколов, с помощью которых производится доступ к сетевым ресурсам. Единицу информации на прикладном уровне называют *сообщением (Message)*.

Прикладные процессы обмениваются информацией с помощью прикладных логических объектов, прикладных протоколов и услуг уровня представления.

Прикладные услуги отличаются от услуг, предоставляемых другими уровнями, тем, что они не предоставляются какому-либо верхнему уровню и не связаны ни с каким пунктом доступа к услугам. Кроме передачи информации может предоставляться следующий набор услуг:

- идентификация партнёров, собирающихся инициировать связь;
- установление уровня авторизации для взаимодействия;
- авторизация партнёров, собирающихся инициировать взаимосвязь;
- определение параметров качества услуг, считающихся приемлемыми;
- идентификация ограничений на синтаксис данных;
- и другие.

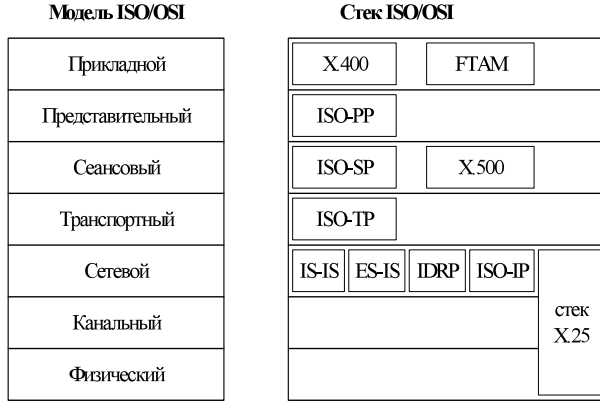

Рис. 2.2. Некоторые протоколы стека ISO/OSI

На прикладном уровне выполняются все функции связи между открытыми системами, которые не выполняются нижележащими уровнями. В их число включаются функции, выполняемые программными средствами, и функции, выполняемые людьми.

2.2. Иерархия протоколов в различных стеках

2.2.1. Стек ISO/OSI

В данном случае эталонная модель первична, а стек протоколов вторичен. Это привело к некоторой тяжеловесности протоколов данного стека (рис. 2.2). Интересно, что большое количество протоколов стека разработано под влиянием IBM.

Из-за ограничений определения *физического уровня* в эталонной модели протоколы физического уровня в данном стеке практически отсутствуют (за исключением семейства протоколов X.25, которое, впрочем, по генезису выбивается из общего построения стека протоколов ISO/OSI).

К *канальному уровню* можно отнести протокол LLC, который хотя и разработан в рамках IEEE 802.2, но служит для сопряжения стека протоколов ISO/OSI с канальным уровнем других стеков.

Основным протоколом *сетевого уровня* является *протокол межсетевого взаимодействия ISO (ISO Internetworking Protocol, ISO-IP)*, описанный в RFC 1575 [1] и документах ISO S 8473, IS 8348. Другое его название — *услуга организации сетевого взаимодействия без установления соединения (Connectionless Network Service, CLNS)*.

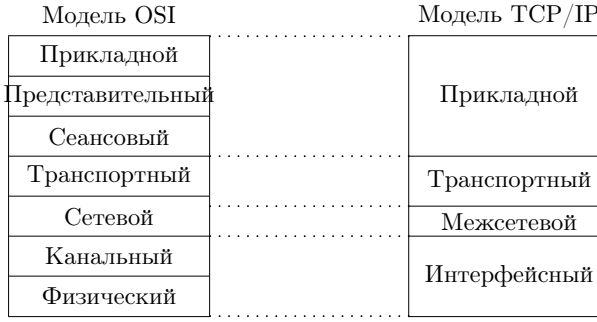

Рис. 2.3. Соответствие эталонных моделей OSI и TCP/IP

Функцию маршрутизации обеспечивают протоколы *IS-IS (Intermediate System to Intermediate System)* (ISO 10589), *ES-IS (End System to Intermediate System)* (ISO 9542) и *CLNS* (ISO 8473), а также *внутридоменный протокол маршрутизации (Inter Domain Routing Protocol, IDRP)* (ISO 7498).

На *транспортном уровне* располагается *транспортный протокол ISO (ISO Transport Protocol, ISO-TP)* (ISO 8073).

Основным протоколом *сеансового уровня* является протокол *ISO-SP (OSI Session Layer Protocol)* (соответствует спецификации ISO/IEC 8327-1 09-1996 ITU-T X.225.) На этом же уровне находится *протокол доступа к каталогам X.500* (прародитель протокола LDAP стека TCP/IP). Кроме того, следует отметить *протокол ISO NetBIOS* (соответствует протоколу NetBIOS одноимённого стека протоколов).

На уровне представления находится *протокол представления (Presentation Protocol, PP)* (ISO IS 8823).

На *прикладном уровне* присутствует набор протоколов, достаточный для основных пользовательских приложений. Здесь же следует упомянуть почтовые протоколы X.400, базирующиеся на рекомендациях CCITT с X.400 по X.430. Стандарт X.400 описывает функционирование *агентов передачи почты (Message Transfer Agents, MTA)*.

Доступ к файлам описывается *протоколом управления доступом и передачей файлов (File Transfer Access and Management, FTAM)* (аналог FTP в стеке TCP/IP). Кроме того, на этом уровне находится сетевой *протокол разделения файлов (Server Message Block, SMB)*.

2.2.2. Стек TCP/IP

Эталонная модель TCP/IP документирует дизайн семейства протоколов TCP/IP и состоит из четырёх уровней (рис. 2.3, 2.4).

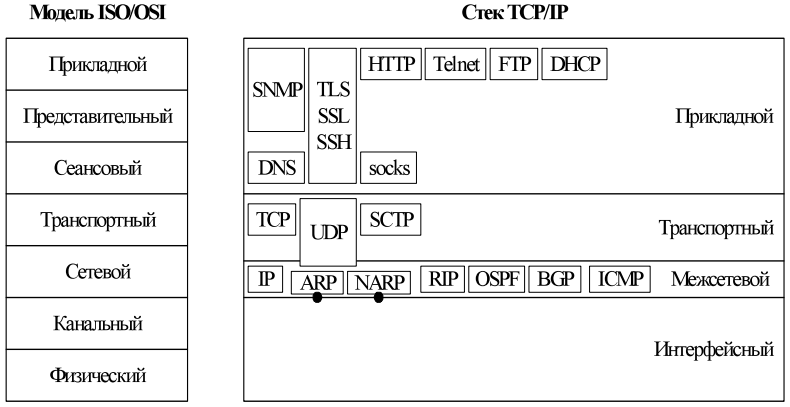

Рис. 2.4. Некоторые протоколы стека TCP/IP

Основой модели служит *межсетевой уровень*. Его задачей является доставка пакетов в пункт назначения. Передача осуществляется без установления соединения. Здесь же осуществляется выбор маршрута пакета. Пакеты могут двигаться к пункту назначения разными маршрутами, поэтому и прибывать они могут не в том порядке, в котором были отправлены.

На межсетевом уровне определён протокол *IP (Internet Protocol)*, задающий в том числе и схему адресации. Кроме того, здесь же определены протоколы маршрутизации *RIP (Routing Information Protocol)*, *OSPF (Open Shortest Path First)*, *BGP (Border Gateway Protocol)*.

Таким образом, межсетевой уровень модели TCP/IP близок сетевому уровню эталонной модели OSI.

На *транспортном уровне* модели TCP/IP решается задача поддержания связи между отправителем и получателем. Этот уровень в основном соответствует транспортному уровню эталонной модели OSI. На нём определены протоколы *TCP (Transmission Control Protocol)*, *UDP (User Datagram Protocol)*, *DCCP (Datagram Congestion Control Protocol)*, *SCTP (Stream Control Transmission Protocol)*.

Прикладной уровень объединяет все службы, представляемые системой пользовательским приложениям. В модели TCP/IP не выделяются отдельно *сеансовый* и *представительный* уровни. Отдельные их функции выполняются различными протоколами прикладного уровня. На этом уровне определены, например, почтовые протоколы *SMTP (Simple Mail Transfer Protocol)*, *IMAP4 (Internet Message Access Protocol rev 4)*, *POP3 (Post Office Protocol version 3)*, протокол передачи гипертекста *HTTP (Hypertext Transfer Protocol)*, протокол передачи файлов *FTP (File Transfer Protocol)*, протокол эмуляции терминала *Telnet* и др.

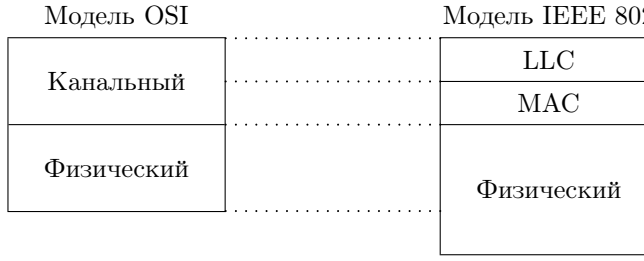

Рис. 2.5. Соответствие эталонных моделей OSI и IEEE 802

Интерфейсный уровень отвечает за взаимодействие между компьютером и физическим сетевым оборудованием. Он приблизительно соответствует канальному и физическому уровням модели OSI. Интерфейсный уровень по-настоящему не описан в документации по архитектуре TCP/IP, в которой сказано только, что он обеспечивает доступ к сетевой аппаратуре системнозависимым способом.

2.2.3. Стек IEEE 802

Семейство протоколов IEEE 802 базируется на фирменных стандартах построения локальных сетей Arcnet, Ethernet, Token Ring.

Протоколы IEEE 802 охватывают только два нижних уровня семиуровневой эталонной модели OSI, а именно физический и канальный (рис. 2.5). Это связано с тем, что именно эти уровни в наибольшей степени отражают специфику локальных сетей.

На *физическом уровне* модели IEEE 802 специфицируются также и различные типы носителей, то есть среда передачи, что не входит в определение физического уровня эталонной модели OSI. Поэтому физический уровень модели IEEE 802 изображён охватывающим область, лежащую ниже физического уровня модели OSI.

В спецификации IEEE *канальный уровень (Data Link Control, DLC)* разделяется на уровень *управления логическим каналом (Logical Linc Control, LLC)* и уровень *управления доступом к носителю (Media Access Control, MAC)*. По сути, уровень MAC эквивалентен всему уровню DLC в предыдущих спецификациях. Добавление уровня LLC является результатом давления IBM, разрабатывавшей стандарт Token Ring одновременно со спецификацией IEEE 802.5. Поэтому уровень LLC — это отражение операций *высокоуровнего протокола управления каналом передачи данных (High-Level Data Link Control, HDLC)* в *системной сетевой архитектуре (Systems Network Architecture, SNA)*.

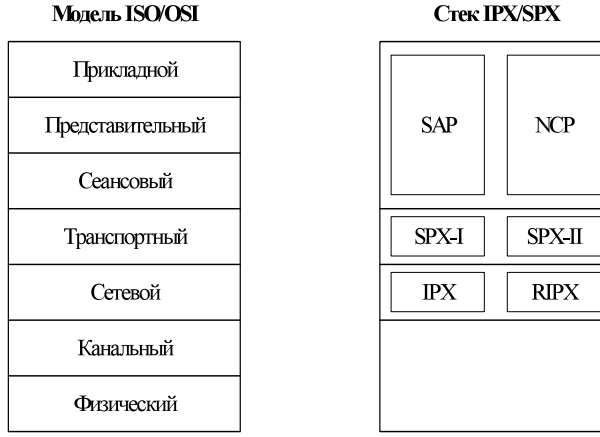

Рис. 2.6. Некоторые протоколы стека IPX/SPX

2.2.4. Стек IPX/SPX

Стек протоколов IPX/SPX (или стек Novell NetWare) разработан в начале 1980-х гг. фирмой Novell для сетевой операционной системы NetWare.

Стек включает в себя следующие протоколы (рис. 2.6): *протокол межсетевого обмена (Interwork Packet Exchange, IPX)*, *протокол маршрутизации (Routing Information Protocol, RIPX)*[1], *протокол упорядоченного обмена пакетами (Sequenced Packet Exchange, SPX)*, *протокол анонсирования сервиса (Service Advertising Protocol, SAP)*, *протокол ядра NetWare (Netware Core Protocol, NCP)* и др.

2.2.5. Стек NetBIOS/SMB

Стек NetBIOS/SMB разработан в 1984 г. совместно IBM и Microsoft для сетей IBM PC Network и IBM Token Ring.

Протокол *NetBIOS (Network Basic Input/Output System)* был разработан как аналог системы BIOS персонального компьютера. Он реализует большинство услуг и функций сетевого, транспортного и сеансового уровней модели ISO/OSI (так, протокол NetBIOS не поддерживает маршрутизацию пакетов, что является одной из основных функций сетевого уровня). Однако впоследствии за протоколом NetBIOS остался только сеансовый уровень, поскольку на более низких уровнях стали использовать стандартные протоколы (например, TCP/IP или IPX/SPX).

[1] Следует различать протокол RIP в стеке TCP/IP и протокол RIPX в стеке IPX/SPX.

Следует отметить, что существует три реализации протокола NetBIOS:
- *NetBEUI (NetBIOS Extended User Interface)* — NetBIOS поверх LLC;
- *NBT (NetBIOS over TCP/IP)* — NetBIOS поверх IP;
- *NetBIOS* — NetBIOS поверх IPX.

Протокол *SMB (Server Message Block)* реализует услуги и функции прикладного уровня и уровня представления модели ISO/OSI. Протокол регламентирует взаимодействие рабочей станции с сервером. В его функции входит создание и разрыв логического соединения между рабочей станцией и сетевыми ресурсами файлового сервера, управление доступом к файлам на файловом сервере, управление очередью печати на сервере печати.

2.2.6. Стек H.323

Стандарт H.323 входит в серию рекомендаций H.32x ITU-T, разработанных для регламентации проведения аудио- и видеоконференций по телекоммуникационным сетям:
- H.320 регламентирует организацию мультимедийной связи по сетям ISDN;
- H.321 регламентирует организацию мультимедийной связи по сетям ATM;
- H.322 регламентирует организацию мультимедийной связи по сетям с коммутацией пакетов с гарантированной пропускной способностью;
- H.323 регламентирует организацию мультимедийной связи по сетям с коммутацией пакетов с негарантированной пропускной способностью;
- H.324 регламентирует организацию мультимедийной связи по телефонным сетям общего пользования;
- H.324/C регламентирует организацию мультимедийной связи по сетям мобильной связи.

По сути, H.323 является набором управляющих протоколов (рис. 2.7), строго регламентирующих использование программ (кодеков) и протоколов других стеков для организации мультимедийной связи по сетям с коммутацией пакетов.

За управление соединением и сигнализацией отвечают следующие протоколы:
- H.225.0 — протокол сигнализации и пакетирования мультимедийного потока;
- H.225.0/RAS — протокол, определяющий процедуры регистрации, доступа и состояния;
- H.245 — протокол управления для мультимедиа.

За безопасность и шифрование отвечает протокол H.235.

Протоколы H.450.x определяют различные дополнительные услуги:
- H.450.1 — определяет функции для управления дополнительными услугами;
- H.450.2 — осуществляет перевод соединения третьему абоненту;
- H.450.3 — осуществляет переадресацию вызова;
- H.450.4 — осуществляет удержание вызова;

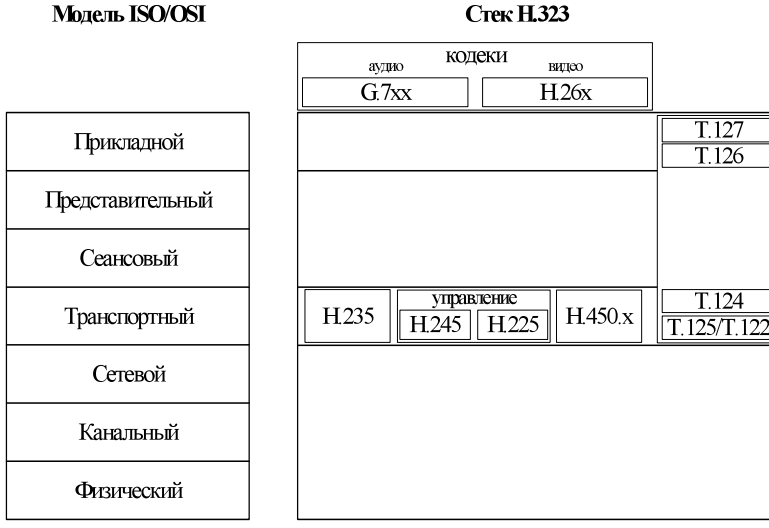

Рис. 2.7. Некоторые протоколы стека H.323

– H.450.5 — осуществляет прикрепление вызова (park) и ответ на вызов (pick up);
– H.450.6 — осуществляет уведомление о вызове в режиме разговора;
– H.450.7 — осуществляет индексацию ожидающего сообщения;
– H.450.8 — осуществляет идентификацию имён;
– H.450.9 — осуществляет завершение соединения.

За организацию конференцсвязи для передачи данных отвечает стек T.120, включающий в себя протоколы T.123, T.124, T.125.

Для обработки аудиосигнала применяются кодеки серии G.7xx: G.711, G.722, G.723.1, G.728, G.729.

Для обработки видеосигнала используются кодеки H.261, H.263, H264.

2.2.7. Стек SS7

Система сигнализации № 7 (SS7 — Signaling System 7, или ОКС7 — система общеканальной сигнализации № 7) разработана и стандартизована ITU-T в 1981 г. и представляет собой набор протоколов сигнализации, предназначенных для обмена информацией управления вызовами между коммутационными станциями и специализированными узлами сетей связи для поддержки как голосовых, так и неголосовых служб [2, 3]. SS7 образует собственную сеть, работающую параллельно цифровой сети связи.

Стек SS7 имеет четыре уровня, соответствующие физическому, канальному, сетевому и прикладному уровням модели ISO/OSI (рис. 2.8).

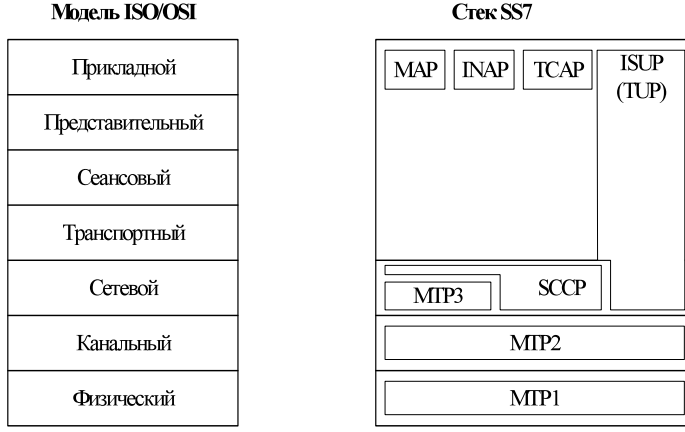

Рис. 2.8. Некоторые протоколы стека SS7

Подсистема передачи сообщений (Message Transfer Part, MTP) состоит из трёх уровней — *MTP1*, *MTP2*, *MTP3*, образующих общую транспортную подсистему, обеспечивающую корректную передачу информации между узлами сети сигнализации.

Уровень MTP1 соответствует физическому уровню модели ISO/OSI. На нём определены физические, электрические и функциональные характеристики звена данных сигнализации и средства доступа к нему.

Уровень MTP2 соответствует канальному уровню модели ISO/OSI. На нём определены функции и процедуры, относящиеся к передаче сигнальных сообщений по отдельному звену сигнализации.

На уровне MTP3 определены процедуры и функции сети сигнализации по маршрутизации сообщений, есть возможность восстановления способности передачи сигнальных сообщений после сбоев в сети, но лишь частично поддерживается адресация. Поэтому данный уровень лишь частично можно соотнести с сетевым уровнем модели ISO/OSI. Соответствие уровней становится полным, если рассматривать данный уровень совместно с *подсистемой управления соединениями сигнализации (Signaling Connection Control Part, SCCP)*.

Подсистемы MTP и SCCP в совокупности образуют *подсистему сетевых услуг (Network Service Part, NSP)*.

Протокол *ISUP (ISDN User Part)* определяет сигнальные функции для установления соединений с возможностью предоставления услуг *цифровой сети с интеграцией служб (Integrated Service Digital Network, ISDN)*. Ранее

функции по управлению вызовами выполняла подсистема *TUP (Telephone User Part)*, впоследствии полностью вошедшая в ISUP. По отношению к модели ISO/OSI ISUP занимает сетевой и прикладной уровни.

На прикладном уровне модели ISO/OSI располагаются прикладная *подсистема обеспечения транзакций (Transaction Capabilities Applications Part, TCAP)*, *подсистема пользовательской мобильной связи (Mobile Application Part, MAP)* и *протокол интеллектуальной сети (Intelligent Network Application Protocol, INAP)*.

Глава 3. Физический уровень

3.1. Модуляция сигналов

Необходимость в модуляции аналоговой информации возникает при передаче низкочастотного (например, голосового) аналогового сигнала через канал, находящийся в высокочастотной области спектра. Для решения этой проблемы амплитуду высокочастотного несущего сигнала изменяют (модулируют) в соответствии с изменением низкочастотного сигнала.

При кодировании цифрового сигнала параметры меняются скачками. Такого рода модуляцию называют *манипуляцией (shift key, SK)*. На рисунке ниже представлены схемы амплитудной (ASK), частотной (FSK) и фазовой (PSK) манипуляций.

Основные технологии модуляции (или кодирования), выполняющие преобразование цифровых данных в аналоговый сигнал:

- амплитудная (Amplitude-Shift Keying, ASK),
- частотная (Frequency-Shift Keying, FSK),
- фазовая (Phase-Shift Keying, PSK).

3.1.1. Амплитудная модуляция

При амплитудной модуляции нулевому биту обычно соответствует нулевое значение амплитуды, единичному биту — некоторое, отличное от нуля, значение амплитуды, т. е. представлению нуля или единицы соответствует наличие или отсутствие соответственно несущей частоты при постоянной амплитуде. Результирующий сигнал при этом имеет вид:

$$s(t) = \begin{cases} A\cos(2\pi f_c t), & \text{кодирует двоичную 1,} \\ 0, & \text{кодирует двоичный 0,} \end{cases}$$

где $A\cos(2\pi f_c t)$ — несущий сигнал; A — амплитуда; f_c — несущая частота; t — время.

3.1.2. Частотная модуляция

Частотная модуляция имеет две формы:

- бинарную (Binary FSK, BFSK),
- многочастотную (Multiple FSK, MFSK).

При бинарной частотной модуляции два двоичных числа представляются сигналами двух различных частот, расположенных около несущей. Результи-

рующий сигнал при этом имеет вид:

$$s(t) = \begin{cases} A\cos(2\pi f_1 t), \\ A\cos(2\pi f_2 t), \end{cases}$$

где $A\cos(2\pi f_c t)$ — несущий сигнал; A — амплитуда; f_1 и f_2 — частоты, смещённые от несущей частоты f_c на величины, равные по модулю, но противоположные по знаку; t — время.

При многочастотной модуляции для кодирования сигнала используется несколько частот, и за один раз пересылается более одного бита. Сигнал при этом имеет вид:

$$s_i = A\cos(2\pi f_i t), \quad 1 \ll i \ll M,$$
$$f_i = f_c + (2i - 1 - M)f_d, \quad M = 2^L,$$

где $A\cos(2\pi f_i t)$ — несущий сигнал; A — амплитуда; f_c — несущая частота; f_d — разностная частота; M — число различных сигнальных посылок; L — количество бит, переданных за один раз; t — время.

Бинарная частотная модуляция менее восприимчива к ошибкам, чем амплитудная модуляция. Многочастотная модуляция эффективнее бинарной, но и более подвержена ошибкам.

3.1.3. Фазовая модуляция

При фазовой модуляции для представления данных выполняется смещение несущего сигнала.

Фазовая модуляция имеет следующие формы:
- двухуровневую (Binary PSK, BPSK),
- дифференциальную (Differential PSK, DPSK),
- квадратурную (Quadrature Phase-Shift Keying, QPSK),
- многоуровневую (Multiple FSK, MFSK).

При двухуровневой фазовой модуляции для представления двух двоичных цифр используются две фазы. При этом результирующий сигнал (для одного периода передачи бита) имеет вид:

$$s(t) = \begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t + \pi) \end{cases} = \begin{cases} A\cos(2\pi f_c t), & \text{кодирует двоичную 1}, \\ -A\cos(2\pi f_c t), & \text{кодирует двоичный 0}, \end{cases}$$

где $A\cos(2\pi f_c t)$ — несущий сигнал; A — амплитуда; f_c — несущая частота; t — время.

При дифференциальной фазовой модуляции для представления двоичного нуля используется сигнал, фаза которого совпадает с фазой предыдущего сигнала, а для представления двоичной единицы — сигнал с фазой, противоположной фазе предыдущего. Такая схема называется *дифференциальной*,

поскольку сдвиг фаз выполняется относительно предыдущего переданного бита, а не относительно какого-то эталонного сигнала.

При квадратурной фазовой модуляции каждой сигнальной посылкой представляется более одного бита, при этом вместо сдвига фазы на π, как в двухуровневой модуляции, используются сдвиги фаз, кратные $\pi/2$:

$$s(t) = \begin{cases} A\cos\left(2\pi f_c t + \dfrac{\pi}{4}\right), & \text{кодирует 11,} \\ A\cos\left(2\pi f_c t + \dfrac{3\pi}{4}\right), & \text{кодирует 10,} \\ A\cos\left(2\pi f_c t + \dfrac{5\pi}{4}\right), & \text{кодирует 00,} \\ A\cos\left(2\pi f_c t + \dfrac{7\pi}{4}\right), & \text{кодирует 01,} \end{cases}$$

где $A\cos(2\pi f_c t)$ — несущий сигнал; A — амплитуда; f_c — несущая частота; t — время.

Схема работы многоуровневой фазовой модуляции аналогична схеме работы квадратурной фазовой модуляции, но в каждый момент времени передаётся по три бита, используется восемь различных углов сдвига фаз, для каждого угла используется несколько амплитуд.

3.1.4. Квадратурная амплитудная модуляция

В современных системах связи большую популярность получила разновидность амплитудной манипуляции QAM (квадратурная). Схема работы квадратурной амплитудной модуляции совмещает в себе принципы амплитудной и фазовой модуляций. На одной несущей частоте одновременно передаются два различных сигнала, но при этом задействованы две копии несущей частоты, сдвинутые относительно друг друга на 90^o (они находятся в квадратуре), и обе несущие являются амплитудномодулированными. Амплитуды этих простых сигналов меняются дискретно, что, в конечном счете, образует сигнал с дискретным изменением и амплитуды и фазы одновременно. В приёмнике эти сигналы демодулируются, а результаты объединяются с целью восстановления исходного двоичного сигнала.

Исходя из таких соображений фазовую манипуляцию можно рассматривать как частный случай квадратурной амплитудной модуляции.

При использовании двухуровневой амплитудной модуляции (2QAM) каждый из двух потоков может находиться в одном из двух состояний, а объединённый поток — в одном из четырёх. При использовании четырёхуровневой модуляции (т.е. четырёх различных уровней амплитуды, 4QAM) объединённый поток будет находиться в одном из 16 состояний. Чем больше число состояний, тем выше скорость передачи данных, возможная при определён-

ной ширине полосы. Но чем больше число состояний, тем выше потенциальная частота возникновения ошибок вследствие помех или поглощения.

3.1.5. Технология расширенного спектра

Основная идея метода состоит в том, чтобы распределить информационный сигнал по широкой полосе радиодиапазона, что в итоге позволит значительно усложнить подавление или перехват сигнала.

3.1.5.1. Расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS)

Передача ведётся с постоянной сменой несущей в пределах широкого диапазона частот. В результате мощность сигнала распределяется по всему диапазону, а прослушивание какой-то определённой частоты даёт только небольшой шум. Последовательность несущих частот псевдослучайна и известна только передатчику и приёмнику. Попытка подавления сигнала в каком-то узком диапазоне почти не ухудшает сигнал, так как подавляется только небольшая часть информации.

На каждой несущей частоте для передачи дискретной информации применяются стандартные методы модуляции — частотная или фазовая. Для синхронизации приёмника и передатчика в течение некоторого времени передаются синхронизирующие последовательности бит. Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Если частота смены подканалов ниже, чем скорость передачи данных в канале, то такой режим называют *медленным расширением спектра*, в противном случае — *быстрым расширением спектра*. Метод быстрого расширения спектра более устойчив к помехам, т.к. помехи, подавляющие сигнал в определённом подканале, не приводят к потере бита, поскольку его значение повторяется несколько раз в различных частотных подканалах. Метод медленного расширения спектра менее устойчив к помехам, но его проще реализовать.

3.1.5.2. Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum, DSSS)

В методе прямого последовательного расширения спектра, в отличие от метода расширения спектра скачкообразной перестройкой частоты, весь частотный диапазон занимается не за счёт постоянных переключений с частоты на частоту, а за счёт того, что каждый бит информации заменяется последовательностью из N бит, что даёт увеличение тактовой скорости передачи сигналов в N раз и соответствующее расширение в N раз спектра сигнала.

Передача двоичной единицы заменяется передачей расширяющей последовательности. Двоичный нуль кодируется инверсным значением расширяющей последовательности. Количество бит в расширяющей последовательно-

сти определяет коэффициент расширения исходного кода. Для кодирования битов результирующего кода может использоваться любой вид модуляции. Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и выше степень подавления помех. Но при этом растёт занимаемый каналом диапазон спектра.

Помехи искажают только определённые частоты спектра сигнала, поэтому приёмник с большой степенью вероятности может правильно распознавать передаваемую информацию.

Метод прямого последовательного расширения спектра в меньшей степени защищён от помех, чем метод быстрого расширения спектра, так как мощные помехи влияют на часть спектра, а значит, и на результат распознавания единиц или нулей.

3.2. Мультиплексирование

При необходимости передачи нескольких потоков данных для одного пользователя или для нескольких приходится решать задачу множественного доступа к середе. Другими словами необходимо так уплотнить потоки или спроектировать такой алгоритм, чтобы лучшим образом организовать связь в имеющихся условиях. В литературе данную проблему именуют и как мультиплексирование и как уплотнение и как множественный доступ (MAC).

Пространственное разделение потоков можно считать относительно простым решением задачи. Примером такого разделения может служить технология *MIMO (Multiple Input Multiple Output)*, которая повсеместно внедряется во все современных стандарты сетей. Суть заключается в использование нескольких антенн, которые разносят друг от друга, чтобы они не мешали передачи. Также наиболее простым примером пространственного разделения может служить ограничение мощности передатчиков или адаптивное изменение диаграмм направленности антенн.

Более распространённой является методика частотного уплотнения или *FDM (Frequency Division Multiplexing)*. Одним из минусов является необходимость между потоками оставлять частотные промежутки, чтобы исключить взаимные помехи, что не лучшим образом использует частотный ресурс.

Более гибкой является техника временного уплотнения или *TDM (Time Division Multiplexing)*. При этом передатчик использует только одну частоту, но для каждого потока используется свой интервал времени. Данная методика очень требовательна к синхронизации между приёмником и передатчиком. TDM удобна для динамичного изменения потоков, например, если какому-нибудь потоку нужно повысить трафик, то достаточно лишь для него сделать интервал подлиннее. Наиболее известным стандартом, использующим TDM, является GSM.

Следует обратить внимание на кодовую методику уплотнения или *CDM (Code Division Multiplexing)*. Потоки сосуществуют в одном частотновременном интервале. Для кодирования каждого потока применяются специальные коды. Коды CDM представляют собой ортогональные сигналы, на которые

раскладываются символы первоначальной последовательности. Это одна из методик уширения спектра.

Существуют различные модификации методики CDM. К примеру, смесь CDM и FMD дают *FHSS (Frequency Hopping Spread Spectrum)*, а с TDM технику *THSS (Time Hopping Spread Spectrum)*. Модификации, обладая уникальными свойствами, открывают широкие горизонты применения CDM. К примеру, FHSS применяется в Bluetooth. Ещё одной производной CDM и FDM является, рассматриваемый в статье, метод OFDM.

Методику уплотнения с целью множественного доступа к среде нескольких пользователей именуют в англоязычной литературе как multiple access, поэтому такие техники называются FDMA, TDMA, CDMA, OFDMA и т.д.

3.2.1. OFDM

В технологии OFDM частотный диапазон разбивается равномерно между поднесущими (называемыми дополнительными несущими), количество которых может доходить до нескольких тысяч. Каждому передаваемому потоку назначается несколько таких поднесущих, т.е. каждый поток разбивается на N поднесущих. Поднесущие между собой ортогональны. Эта особенность определяет многие положительные качества техники OFDM.

Для борьбы с помехами в OFDM включён защитный интервал. Это возможно сделать, т.к. быстрый поток данных делится между поднесущими, на каждой из которых скорость подпотока меньше первоначальной. За счёт этого можно выделить отрезок времени, который будет защищать основной сигнал от помех. Длительность этого защитного интервала может составлять $1/4$, $1/8$, $1/16$ или $1/32$ от длительности OFDM символа.

Межсимвольная интерференция является одной из разновидностей помех, она появляется в результате взаимодействия пакетов передаваемых данных, например, вследствие многолучевого распространения сигнала, вызванного переотражением. Обычно в качестве защитного интервала используют так называемый циклический префикс, являющийся копией окончания сигнала размещённой впереди. Это позволяет сохранить ортогональность. Чем дольше защитный интервал, тем в более сложных условиях может передаваться OFDM сигнал.

Ортогональность поднесущих позволяет системам хорошо справляться с узкополосными помехами, которые могут подавить часть поднесущих. Благодаря корректирующим кодам информацию можно извлечь из неповреждённых поднесущих. Помимо этого, в OFDM каждая поднесущая может модулироваться различной схемой модуляции, например, QPSK, 16-QAM или 64-QAM. В таком подходе можно адаптивно регулировать помехоустойчивость и скорость потока данных для каждого канала в отдельности.

Технической реализации OFDM не было долгое время, поскольку решение задачи аналоговыми методами весьма проблематично. С появлением быстрых вычислительных систем задача была реализована с помощью цифровых методов обработки сигналов. В основе подхода лежит преобразование

Фурье, а точнее алгоритм быстрого преобразования Фурье. Синтетическим методом создаётся спектр сигнала, из которого обратным быстрым преобразованием Фурье (IFFT) получается аналоговый сигнал. Спектр такого сигнала уже состоит из ортогональных поднесущих, этот факт получается по определению преобразования Фурье.

Непосредственное формирование сигнала после цифрового синтеза, который затем передаётся в антенну для излучения, происходит аналогично схеме QAM модуляции. В отдельности формируются квадратурные сигналы как мнимая и реальная часть синтезируемого сложного сигнала, а затем происходит его сборка и передача.

3.2.1.1. Виды OFDM

Ниже приведён список различных модификаций технологии OFDM, которые можно встретить в литературе.

- COFDM (Coded OFDM). Данный вид OFDM отличается лишь тем, что данные предварительно кодируются корректирующими кодами. В DVB-T кстати, используется именно этот вид OFDM.
- Flash OFDM (Fast low-latency access with seamless handoff OFDM). Эта модификация была разработана компанией Flarion Technologies и предназначена для мобильных устройств. Все особенности модификации заключаются в алгоритмах работы с коммутацией пакетов данных.
- OFDMA. Это многопользовательский вариант OFDM технологии.
- VOFDM (Vector OFDM). Данную модификацию курирует компания Cisco Systems . В основе лежит концепция технологии MIMO. Сюда же можно отнести MIMO-OFDM.
- WOFDM (Wideband OFDM). Широколопосная модификация OFDM разработанная Wi-LAN Inc . В модификации достигается повышение пропускной способности и помехоустойчивости. Основное отличие в большем частотном расстояние между несущими.

Среди рассмотренных систем большую популярность получили классическая OFDM схема и COFDM модификация.

3.3. Кодирование сигнала

Одной из основных задач физического уровня модели OSI является преобразование данных в электромагнитные сигналы, и наоборот. Переход от электромагнитых импульсов к последовательности бит называют *кодированием сигнала*.

Рассмотрим наиболее распространённые методы кодирования (рис. 3.1).

3.3.1. Код NRZ и NRZI

Код *NRZ (Non Return to Zero)* — простейший двухуровневый код. Логической единице соответствует верхний уровень, логическому нулю — нижний,

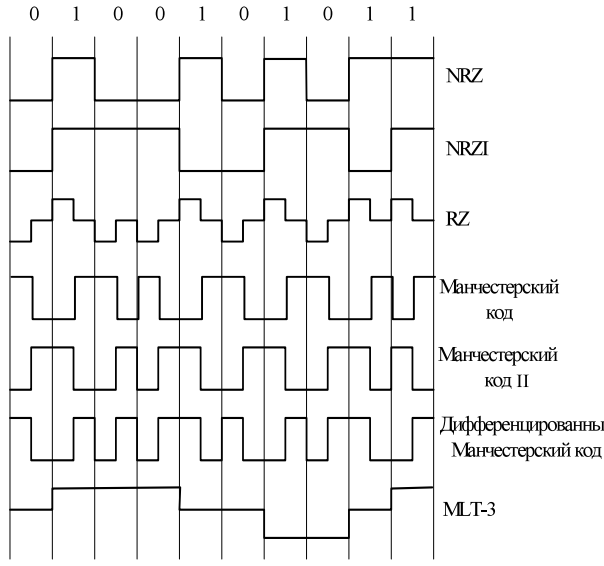

Рис. 3.1. Методы кодирования сигнала

переходы электрического сигнала происходят на границе битов (рис. 3.2). Код NRZ отличается простотой и обеспечивает высокую скорость передачи, но не имеет синхронизации.

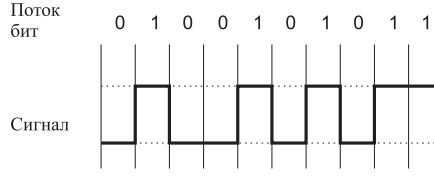

Рис. 3.2. Код NRZ

Код *NRZI (Non Return to Zero Invert to ones)* представляет собой модификацию кода NRZ. В этом двухуровневом коде принимается во внимание значение предыдущего бита. Уровень сигнала меняется, если текущий бит — единица, и повторяет предыдущий, если текущий бит имеет значение 0 (рис. 3.3). NRZI используется в основном для работы с оптоволоконной средой, в сетях

100Base-FX.

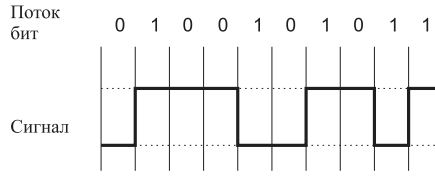

Рис. 3.3. Код NRZI

3.3.2. Код Rz

Код *RZ (Return to Zero)* обеспечивает возвращение к нулю после передачи каждого бита информации. RZ — трёхуровневый код. В центре бита всегда есть переход. Логической единице соответствует отрицательный импульс, логическому нулю — положительный (рис. 3.4). RZ — самосинхронизирующийся код, однако, он не даёт выигрыша в скорости. Код RZ нашёл применение в оптоволоконных сетях.

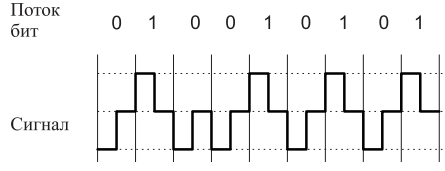

Рис. 3.4. Код Rz

3.3.3. Манчестерский код

Двухуровневый Манчестерский код широко используется в локальных сетях. Логической единице соответствует переход вниз в центре бита, логическому нулю — переход вверх (рис. 3.5). Манчестерский код является самосинхронизирующимся и обладает хорошей помехозащищённостью.

3.3.4. Код MLT-3

Код *MLT-3 (Multi Level Transmission-3)* — трёхуровневый код. Как и в NRZI, логической единице соответствует смена уровня сигнала, а при передаче нуля сигнал не меняется (рис. 3.6). Изменение уровня сигнала происходит

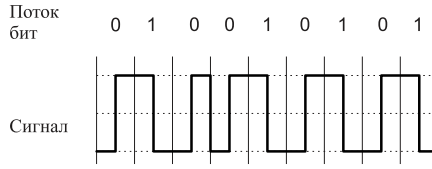

Рис. 3.5. Манчестерский код

последовательно с учётом предыдущего перехода. Основной недостаток кода MLT-3 — отсутствие синхронизации. MLT-3 применяется в сетях 100Base-T на основе витой пары.

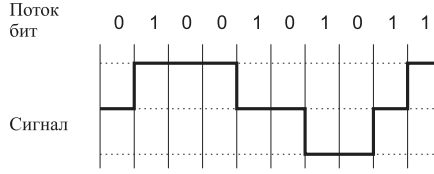

Рис. 3.6. Код MLT-3

Глава 4. Канальный уровень

4.1. Доступ к среде

При доступе к среде возникает проблема распределения одного широковещательного канала между несколькими пользователями. Можно выделить две схемы выделения канала: *статическую* и *динамическую*. Рассмотрим динамическое выделение канала.

4.1.1. Динамическое выделение канала

Рассмотрим вначале несколько моделей.

1. *Многостанционная модель*. В рамках этой модели рассматривается N независимых станций, каждая из которых порождает кадры с вероятностью $\lambda\Delta t$ за период Δt, где λ — некоторый параметр. После отправки кадра станция блокируется и ничего не предпринимает, пока кадр не будет успешно передан.
2. *Модель единого канала*. Для всех коммуникаций используется один канал. Все станции эквивалентны.
3. *Модель с коллизиями*. Если два кадра передаются одновременно, они перекрываются и возникает коллизия. Все станции могут детектировать коллизии. Эти кадры должны быть переданы ещё раз. За исключением коллизий, других ошибок нет.
4. *Временны́е модели*:
   (a) *Модель непрерывного времени*. Передача кадров может произойти в любой момент времени. Время непрерывно.
   (b) *Модель тактированного времени*. Время разбивается на дискретные интервалы — *такты (Slots)*. Передача кадров происходит всегда в начальный момент такта.
5. *Модели с несущей*:
   (a) *Модель с прослушиванием несущей*. Прежде чем использовать канал, станции запрашивают состояние канала. Если он занят, то все станции перестают его использовать до тех пор, пока он не освободится.
   (b) *Модель без прослушивания несущей*. Станции не запрашивают состояние канала перед началом передачи.

4.1.2. Протоколы множественного доступа

Рассмотрим некоторые модели протоколов с множественным доступом.

4.1.2.1. Семейство протоколов ALOHA

В 1970-х гг. в Гавайском университете под руководством Нормана Абрамсона была разработана система ALOHA. Она использовалась для наземной системы радиодоступа.

Центральный узел, называемый базовой станцией, принимает пакеты, передаваемые другими узлами на частоте $f_0 = 417$ МГц и ретранслирует эти пакеты на частоте $f_1 = 413$ МГц. Узлы сети ALOHA передавали пакеты со скоростью 9600 бит/с.

Узлы передают пакеты по общему каналу. Когда передача двух пакетов происходит одновременно, они искажают друг друга. Возникают коллизии. В начальной реализации сети ALOHA центральный узел подтверждает верно принятые пакеты. Когда узел не получает подтверждение за определённый промежуток времени, он полагает, что произошла коллизия, и передаёт пакет снова.

ALOHA не использует контроль несущей и не прекращает передачу пакета при обнаружении конфликта. Контроль несущей бесполезен, поскольку узлы расположены далеко друг от друга, и узел может завершить передачу прежде, чем другой узел заметит передачу. По тем же причинам обнаружение конфликтов слишком запаздывает.

Рассмотрим две версии протокола ALOHA: *чистую (Pure ALOHA)* и *тактированную (синхронную) (Slotted ALOHA)*. В первой используется модель непрерывного времени, а во второй — тактированного.

В модели *Чистая ALOHA* станция начинает передачу данных сразу же, как только у неё появляются данные. При возникновении коллизии посылающая станция ждёт случайный промежуток времени, а затем повторяет передачу этого кадра.

Таким образом, если станция начала передачу в то время, пока предыдущий кадр находится в канале, возникает коллизия. Оба пакета разрушаются и должны быть переданы повторно.

В модели *Тактированная ALOHA* время разбивается на дискретные интервалы. Передача может начаться только в начале такта. Когда у узла появляется новый пакет, он осуществляет его передачу в начале следующего такта. Если в течение этого временного интервала передаётся только один пакет, то передача является успешной. В противном случае возникает коллизия, и узел осуществляет повторную передачу через случайный период времени.

Для реализации тактированной версии протокола ALOHA необходимо приведение узлов к общему эталону времени для определения начала временны́х интервалов.

4.1.2.2. Протоколы множественного доступа с контролем несущей

Протоколы, в которых станции контролируют несущую, называются *протоколами с контролем несущей (Carrier Sense, CS)*.

Рассмотрим несколько видов протоколов семейства *CSMA (Carrier Sense Multiple Access)*.

1-устойчивый (1-persistent) CSMA. Когда станция готова к передаче данных, она прослушивает канал, чтобы определить, не передаёт ли данные кто-либо другой. Если канал занят, станция ждёт, когда он освободится. Если же канал свободен, станция передаёт информацию. При возникновении коллизии станция ждёт случайный промежуток времени, а потом продолжает действовать по вышеописанному алгоритму. Протокол называется 1-устойчивый, потому что в случае свободного канала станция осуществляет передачу с вероятностью 1.

Неустойчивый (nonpersistent) CSMA. Этот случай немного отличается от предыдущего. Здесь опять перед передачей данных станция прослушивает канал. Но в случае, когда канал уже используется, станция ожидает случайный период времени и повторяет алгоритм.

p-устойчивый (p-persistent) CSMA. Данный вид применяется к тактированному каналу. Если канал свободен, то передача осуществляется с вероятностью p. Соответственно с вероятностью $q = 1 - p$ станция будет ждать следующего такта. Если канал свободен, то передача данных или ожидание следующего такта происходят с вероятностью p и q соответственно. Этот процесс продолжается до тех пор, пока либо кадр не будет передан, либо другая станция не начнёт передачу. В последнем случае возникает коллизия; станция ожидает случайный период времени и пытается снова осуществить передачу данных. Если же при прослушивании канала он оказывается занятым, то станция ждёт до начала следующего такта и повторяет алгоритм.

Устойчивый и неустойчивый CSMA являются непосредственным улучшением протоколов семейства ALOHA, поскольку в них для определения состояния канала осуществляется его прослушивание.

Протоколы множественного доступа с контролем несущей с определением коллизий (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) являются дальнейшим улучшение протоколов, рассмотренных в предыдущем пункте. Здесь при возникновении коллизии станции сразу же прекращают передачу данных (вместо того, чтобы продолжать передачу, что бессмысленно). Это позволяет сэкономить и время, и полосу пропускания.

При обнаружении коллизии станция прекращает передачу данных и ждёт случайное время. По истечении данного времени станция опять пытается передать данные.

Разберём алгоритм определения коллизий подробнее. Пусть две станции начали передачу данных в один и тот же момент времени. Время определения коллизии будет зависеть от времени распространения сигнала между двумя этими станциями.

Обозначим через τ время прохождения сигнала между двумя наиболее удалёнными друг от друга станциями. Пусть первая станция начинает передачу данных в некоторый момент времени t_0. Если в промежуток времени $[t_0, t_0 + \tau)$ вторая станция тоже начнёт передачу, то она обнаружит коллизию. Чтобы коллизию обнаружила и первая станция, сигнал должен вернуться обратно, то есть коллизия будет обнаружена в промежуток времени $[t_0, t_0 + \tau)$. Временной интервал 2τ называется *временем двойного оборота (Path Delay*

Value, PDV).

4.2. Технологии региональных сетей

Региональные сети строятся по принципу функционального разделения по уровням доступа: опорная сеть (магистраль), уровень распределения/агрегации, уровень доступа (клиентский доступ).

4.2.1. Технологии опорной сети

Опорная сеть обычно имеет кольцевую топологию, обеспечивающую резервирование и повышенную надёжность. В качестве физической среды передачи данных применяется оптоволокно. Базовыми магистральными технологиями являются SONET/SDH, ATM, POS (Pocket over Sonet), EoSDH (Ethernet over SDH), DWDM, CWDM, DPT/RPR, Fast/Gigabit/10 Gigabit Ethernet.

На уровне доступа применяются следующие технологии: Ethernet (Ethernet, Fast Ethernet, Gigabit Ethernet), LRE, xDSL (HDSL, ADSL, VDSL, SDSL), PNA (Phoneline Networking Alliance), Wireless (802.11), Infrared, PON (Passive Optical Network), EFM (Ethernet in the First Mile, IEEE 802.3ah), Satellite.

Для обеспечения повышенной надёжности и резервирования широко используется топологическая модель кольца. Кольца обычно создают на уровнях опорной сети и доступа.

4.2.1.1. SONET/SDH

Изначально основной задачей телекоммуникационных структур являлась передача голосового трафика. Скорость передачи данных задаётся относительно звука с *импульсной модуляцией (Pulse Code Modulation, PCM)* с частотой дискретизации 8 кГц и 8-битной дискретизацией. В результате получается *базовый поток (Digital Signal, DS0)* 64 Кбит/с. Потоки агрегируются и передаются по высокоскоростным каналам. Агрегирование происходит по *технологии временного мультиплексирования каналов (Time Division Multiplexing, TDM)*. Непосредственное слияние и разделение каналов производят специальные устройства — *мультиплексоры*. Например, на вход мультиплексора может поступать 30 потоков DS0 (64 Кбит/с × 30 + 2 сигнальных по 64 Кбит/с), а на выходе получается один E1 (2048 Кбит/с).

В свою очередь, для мультиплексирования потоков информации при формировании мощных региональных и межрегиональных каналов были разработаны стандарты для высокоскоростных оптических сетей связи — сначала *плезиохронная цифровая иерархия (Plesiochronous Digital Hierarchy, PDH)*, а затем и более совершенная *синхронная цифровая иерархия (Synchronous*

Digital Hierarchy, SDH), распространённая в Европе, и её американский аналог *SONET*.

SONET/SDH предполагает использование метода временно́го мультиплексирования и синхронизацию временны́х интервалов трафика между элементами сети и определяет уровни скоростей прохождения данных и физические параметры. Основными устройствами являются мультиплексоры, а физической средой передачи — оптоволокно. При построении сети SDH обычно используется топология двойного кольца. По одному кольцу передаётся синхронизирующая информация, а по другому — непосредственно трафик. Использование колец даёт возможность автоматического восстановления при авариях. Метод передачи — коммутирование каналов.

К достоинствам SONET/SDH относят:

- стандартизованность,
- масштабируемость,
- высокую надёжность (время восстановления порядка 50 мс).

К недостаткам SONET/SDH относят:

- ориентацию на передачу голосового трафика,
- фиксированную полосу пропускания, не зависящую от загрузки каналов,
- неэффективное использование колец.

SONET/SDH является самой зрелой и поэтому самой распространённой на данный момент технологией для построения магистральных каналов передачи данных. Основная область её применения — первичные сети операторов связи. Мультиплексоры, объединённые оптическими линиями связи, образуют единую среду, в которой прокладываются цифровые каналы между оборудованием телефонных сетей или сетей передачи данных. Кроме того, технология SONET/SDH может являться транспортной основой для более современных протоколов, таких как ATM, POS и MPLS.

4.2.1.2. ATM

Как решение проблемы создания мультисервисной и высокоскоростной технологии передачи данных была предложена *технология асинхронной передачи данных (Asynchronous Transfer Mode, ATM)*. В локальных сетях ATM распространения не получила, но до сих пор применяется при построении магистральных сетей. ATM может работать поверх SONET/SDH.

Технология ATM представляет собой транспортный механизм коммутации ячеек небольшого размера фиксированной длины (53 байта). Наиболее распространённая среда передачи для ATM — оптоволокно.

В ATM при соединении создаётся виртуальный канал. Далее коммутация ячеек происходит на основе идентификаторов виртуального канала (VPI/VCI), присутствующих в заголовках.

ATM имеет встроенную поддержку обеспечения гарантированного качества обслуживания.

4.2.1.3. POS

Для решения проблемы накладных расходов в случае передачи IPтрафика через сети SONET/SDH с использованием ATM была разработана технология *POS (Packet Over Sonet/SDH)*, непосредственно инкапсулирующая данные в кадры SDH. Практически получается интерфейс с IPадресом, который использует все преимущества транспортной оптической технологии, не задействуя никаких промежуточных протоколов.

4.2.1.4. EoSDH

Отвечая потребностям рынка по передаче непосредственно Ethernet трафика по наследованным оптическим сетям, появилась технология Ethernet over SONET/ SDH. Вначале допускались только соединения типа точка-точка, затем возникли и многоточечные каналы.

4.2.1.5. WDM

Непрерывно возрастающие объёмы трафика требуют повышения пропускной способности оптических магистралей. Кроме тривиального повышения скоростей передачи существует и другой способ решения данной задачи — уплотнение (мультиплексирование) каналов. Наиболее развитой в настоящее время является *технология оптического спектрального уплотнения*, называемая обычно *мультиплексированием с разделением по длине волны (Wavelength Division Multiplexing, WDM)*.

Принцип работы WDM следующий. Потоки данных от отдельных источников переносятся световыми волнами разной длины (каждому каналу принадлежит своя длина) и объединяются мультиплексором в единый многочастотный сигнал, который передаётся по оптическому волокну. На стороне приёмника происходит обратное преобразование.

Технология WDM соответствует физическому уровню сетевых взаимодействий и работает независимо от типа и формата передаваемых данных, то есть является протокольнонезависимой. К WDM мультиплексору можно подключить практически любое оборудование: SONET/SDH, ATM, Ethernet.

WDM бывает двух видов: *плотное волновое мультиплексирование (Dense Wavelength Division, DWDM)* и *грубое волновое мультиплексирование (Coarse Wavelength Division, CWDM)*.

DWDM может обеспечить большое число спектральных каналов на одно оптоволокно (32, 64 или даже 128). Отсюда её основная отличительная особенность — малые расстояния между мультиплексными каналами.

CWDMсистемы рассчитаны на меньшее число каналов (4, 8 или 16). Поэтому в них спектры соседних информационных каналов расположены на гораздо больших расстояниях друг от друга, чем в DWDM. Скорости передачи CWDM систем ниже, чем у DWDM.

4.2.1.6. DPT/RPR

Стандарт IEEE 802.17 (вобравший в себя DPT/RPR) позиционируется как высокоскоростная технология динамической передачи IP-пакетов, предназначенная для решения задач построения региональных сетей.

В DPT/RPR (IEEE 802.17) к IP-пакету добавляется прослойка второго уровня (MAC), пакет помещается в произвольную физическую оптическую среду (SONET/ SDH, WDM) с топологией двойного кольца. Данные одновременно передаются по двум кольцам в противоположных направлениях. Поток данных в каждом кольце включает непосредственно транспортируемые в данном кольце данные и управляющие пакеты для соседнего кольца.

Достоинства:

- пакетно-ориентирован;
- не требуется дополнительная прослойка типа ATM для доступа к физической оптической среде;
- заложен высокий уровень резервирования и быстрая восстановимость в случае аварий (50 мс);
- эффективно используется ёмкость оптических каналов за счёт смешения контрольных и передаваемых данных.

4.2.2. Технологии уровня доступа

Существует широкий спектр решений для обеспечения абонентского доступа (так называемая ”<первая/последняя миля”>): Ethernet (Ethernet, Fast Ethernet, Gigabit Ethernet), LRE, xDSL (HDSL, ADSL, VDSL, SDSL), PNA (Phoneline Networking Alliance), Wireless (802.11), Infrared, PON (Passive Optical Network), EFM (Ethernet in the First Mile alliance 802.3ah), Satellite.

4.2.2.1. VLAN

Для построения развитых Ethernet сетей используют *технологию виртуальных локальных сетей (Virtual Private Lan, VLAN)* (IEEE 802.1Q), которая позволяет создавать в едином Ethernetсегменте независимые логические области, ограничивающие на канальном уровне распространение трафика (в том числе и широковещательного). В заголовок Ethernetфрейма вводится дополнительная информация о принадлежности к влану (VLAN); получается помеченный кадр данных (Tagged Vlan), который передаётся по транковым линиям (802.1Q Trunk). Это позволяет передавать по одному каналу данные нескольких изолированных локальных сетей. Дальнейшая коммутация происходит с учётом 802.1Qметки. На выходе из коммутатора (например, на стороне клиентского порта) метка (Tag) убирается, что называется *вхождением порта в нетагированный влан (Untagged Vlan)*.

Обычно клиентские подсети изолируются друг от друга путём подключения к раздельным вланам (через порты с Untagged Vlan), а связь между ними организуется при помощи маршрутизатора через 802.1Q транки.

На практике использование вланов даёт возможность гибко изменять логическую организацию сети независимо от реальной физической топологии.

4.2.2.2. Q-in-Q

Непосредственным решением присущих 802.1Q вланам ограничений (например, их максимальное число 4096) явилась технология Q-in-Q. Операторское устройство, получающее клиентский кадр Ethernet, добавляет ещё одну 802.1Qметку, которая и принимается во внимание при дальнейшей коммутации. Так получается целый блок меток, а сам процесс называется *стекированием вланов (802.1Q stacking)*. На выходе из провайдерской сети дополнительная метка удаляется. Это позволяет строить полностью прозрачные на канальном уровне сети.

4.2.2.3. STP

В сетях Ethernet коммутаторы поддерживают только древовидные связи (ациклический граф). Отказоустойчивость требует наличия петель (циклический граф). Технология STP (Spanning Tree Protocol) позволяет совместить оба требования.

После активирования коммутаторы обмениваются специальными информационными пакетами (BPDU), с помощью которых вначале выбирается корневой мост (который будет в итоге находиться на вершине древовидной структуры), а затем кратчайшие (в смысле пропускной способности) пути от каждого из коммутаторов до корневого. В конечном итоге формируется логическая беспетельная топология путём блокирования некоторых избыточных связей.

Расширением STP является стандарт *RSTP (Rapid Spanning Tree Protocol)*.

4.2.3. Технология Metro Ethernet

Преимущества Ethernet: высокая скорость, лёгкость масштабирования технологии, простота для массового использования.

Первоначально Ethernet строилась на базе разделяемой среды передачи, но позднее был введён коммутируемый Ethernet. Были созданы механизмы, гарантирующие качество обслуживания, что дало возможность использовать Ethernet для передачи мультимедийных данных.

Развитием технологии Ethernet для региональных сетей занимается *Metro Ethernet Forum (MEF)* — некоммерческая организация, созданная для продвижения концепции построения операторских сетей на основе Ethernet и ускорения их развёртывания во всём мире. В октябре 2003 г. форум Metro Ethernet ратифицировал первый стандарт, описывающий службы Metro Ethernet: MEF Technical Specification—Ethernet Services Model Phase 1.

По сравнению с технологиями, имеющими схожие потребительские свойства, например SDH/SONET, реализация Metro Ethernet обходится в среднем

в 2–3 раза дешевле. В настоящее время все серьёзные поставщики оборудования выпускают оборудование для Metro Ethernet и ведут активную маркетинговую политику по его продвижению на рынке.

Форум Metro Ethernet предложил модель услуг Metro Ethernet. В основе базовой модели лежит *городская Ethernetсеть (Metro Ethernet Network, MEN)*, принадлежащая провайдеру. *Клиентское оборудование (Customer Equipment, CE)* подключается к сети с помощью интерфейса UNI (User Network Interface), который представляет собой стандартный Ethernet.

Для потребителя существует только Ethernet-интерфейс (UNI), которым он подключается к провайдеру услуг. Транспортные технологии, обеспечивающие работу Metro Network, для него скрыты.

Ключевым элементом модели является *виртуальное соединение Ethernet (Ethernet Virtual Connection, EVC)*, которе определяется как соединение двух и более UNI. По ним проходят данные в виде кадров Ethernet. EVC выполняет две функции:

- соединяет UNI потребителей и пропускает между ними Ethernetфреймы; обеспечивает защищённость и безопасность;
- доставка кадров Ethernet производится с неизменяемыми параметрами: MAC-адреса и содержимое не изменяются в отличие от маршрутизирующих сетей.

MEF определяет два типа EVC: *один-к-одному (Point-to-Point)* и *многие-ко-многим (Multipoint-to-Multipoint)*.

MEF определяет два типа базовых услуг Ethernet: *E-Line (Ethernet Line service type)* и *E-LAN (Ethernet LAN service type)*:

- E-Line обеспечивает соединения point-to-point (аналог физических выделенных каналов или виртуальных выделенных каналов Frame Relay);
- E-LAN поддерживает multipoint соединения (подобен услуге прозрачных локальных сетей (TLS)).

Для полного определения сервисов провайдер услуг должен обозначить кроме типа сервиса (E-Line или E-LAN) на основе EVC ещё и атрибуты, которые можно сгруппировать по категориям:

- *физический интерфейс (Ethernet Physical Interface)* определяет параметры физического уровня модели OSI;
- *параметры трафика (Traffic Parameters)* определяют полосу пропускания;
- *дополнительные параметры качества трафика (Perfomance Parameters)*: доступность (Availability), задержка (Delay), джиттер (Jitter), потери (Loss);
- *классы обслуживания (Class of Service)*;
- *необходимость доставки служебных пакетов (Service Frame Delivery)*;
- *поддержка VLAN (Vlan Tag Support)*: 802.1q, Q-in-Q, MAC-in-MAC;
- *фильтры (Security Filters)*: разнообразная фильтрация фреймов на основе различных критериев;
- *мультиплексирование виртуальных соединений (Service multiplexing)*: поддержка нескольких EVC на одном UNI;

– *неизменность клиентских VLAN (Vlan Transparency)*: неизменность клиентских вланов CE-Vlan при переходе через UNI, т.е. входной CE-Vlan и выходной CE-Vlan для одного и того же EVC одни и те же;
– *связывание (Bundling)*: отображение нескольких вланов CE-Vlan на одно EVC (используя Q-in-Q).

4.3. Технологии беспроводного доступа

4.3.1. Методы доступа к среде в беспроводных сетях

Существует несколько базовых методов доступа (их ещё называют методами уплотнения или мультиплексирования), основанных на разделении между станциями таких параметров, как пространство, время, частота и код. Задача уплотнения — выделить каждому каналу связи пространство, время, частоту и/или код с минимумом взаимных помех и максимальным использованием характеристик передающей среды.

4.3.1.1. Уплотнение с пространственным разделением

Основано на разделении сигналов в пространстве, когда передатчик посылает сигнал, используя код c, время t и частоту f области s_i. То есть каждое беспроводное устройство может вести передачу данных только в границах определённой территории, на которой любому другому устройству запрещено передавать свои сообщения.

4.3.1.2. Уплотнение с частотным разделением (Frequency Division Multiplexing, FDM)

Каждое устройство работает на определённой частоте, благодаря чему несколько устройств могут вести передачу данных на одной территории. Это один из наиболее известных методов, так или иначе используемый в самых современных системах беспроводной связи.

Эта схема приводит к неоправданному расточительству частотных ресурсов, поскольку требует выделения своей частоты для каждого беспроводного устройства.

4.3.1.3. Уплотнение с временны́м разделением (Time Division Multiplexing, TDM)

В данной схеме распределение каналов идёт по времени, т. е. каждый передатчик транслирует сигнал на одной и той же частоте, но в различные промежутки времени (как правило, циклически повторяющиеся) при строгих требованиях к синхронизации процесса передачи.

Временны́е интервалы могут динамично перераспределяться между устройствами сети. Устройствам с большим трафиком назначаются более длительные интервалы, чем устройствам с меньшим объёмом трафика.

Основной недостаток систем с временны́м уплотнением — мгновенная потеря информации при срыве синхронизации в канале, например из-за сильных помех, случайных или преднамеренных.

4.3.1.4. Уплотнение с кодовым разделением (Code Division Multiplexing, CDM)

В данной схеме все передатчики транслируют сигналы на одной и той же частоте.

В схеме CDM каждый передатчик заменяет каждый бит исходного потока данных на CDMсимвол — кодовую последовательность длиной в 11, 16, 32, 64 и т. п. бит (так называемый чип). Кодовая последовательность уникальна для каждого передатчика.

Приёмник знает CDM-код передатчика, сигналы которого должен воспринимать. Он постоянно принимает все сигналы и оцифровывает их. Затем в специальном устройстве (корреляторе) производится операция свёртки (умножения с накоплением) входного оцифрованного сигнала с известным ему CDM-кодом и его инверсией. В несколько упрощённом виде это выглядит как операция скалярного произведения вектора входного сигнала и вектора с CDM-кодом. Если сигнал на выходе коррелятора превышает некий установленный пороговый уровень, приёмник считает, что принял 1 или 0. Для увеличения вероятности приёма передатчик может повторять посылку каждого бита несколько раз. При этом сигналы других передатчиков с другими CDM-кодами приёмник воспринимает как аддитивный шум. Благодаря большой избыточности мощность принимаемого сигнала может быть сопоставима с интегральной мощностью шума. Сходства CDM-сигналов со случайным (гауссовым) шумом добиваются, используя CDM-коды, порождённые генератором псевдослучайных последовательностей. Этот метод также называется *методом расширения спектра сигнала посредством прямой последовательности (Direct Sequence Spread Spectrum, DSSS)*.

Наиболее сильная сторона данного уплотнения заключается в повышенной защищённости и скрытности передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев и обнаружить его присутствие. Кроме того, кодовое пространство более значительно по сравнению с частотной схемой уплотнения, что позволяет без особых проблем присваивать каждому передатчику свой индивидуальный код.

4.3.1.5. Механизм мультиплексирования посредством ортогональных несущих частот (Orthogonal Frequency Division Multiplexing, OFDM)

Весь доступный частотный диапазон разбивается на достаточно много поднесущих (от нескольких сот до тысяч). Одному каналу связи (приёмнику и

передатчику) назначают для передачи несколько таких несущих, выбранных из множества по определённому закону. Передача ведётся одновременно по всем поднесущим, т.е. в каждом передатчике исходящий поток данных разбивается на N субпотоков, где N — число поднесущих, назначенных данному передатчику. Распределение поднесущих в ходе работы может динамически изменяться.

Преимущества:

- Селективному замиранию будут подвержены только некоторые подканалы, а не весь сигнал. Если поток данных защищён кодом прямого исправления ошибок, то с этим замиранием легко бороться.
- OFDM позволяет подавить межсимвольную интерференцию. Межсимвольная интерференция оказывает значительное влияние при высоких скоростях передачи данных, так как расстояние между битами (или символами) мало. В схеме OFDM скорость передачи данных уменьшается в N раз, что позволяет увеличить время передачи символа в N раз. Таким образом, если время передачи символа для исходного потока составляет T_s, то период сигнала OFDM будет равен NT_s. Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы N выбирается таким образом, чтобы величина NT_s значительно превышала среднеквадратичный разброс задержек канала.

4.3.2. Стек протоколов IEEE 802.11 (WiFi)

Стандарты IEEE 802.11 (WiFi, Wi-Fi, Wireless Fidelity)[1] описывают *беспроводную технологию локальных сетей (Wireless Local Area Network, WLAN)*.

Сети WLAN имеют ряд преимуществ перед обычными кабельными сетями:

- их можно быстро развернуть;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорость современных сетей довольно высока (до 108 Мбит/с), что позволяет использовать их для решения очень широкого спектра задач;
- может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Вместе с тем беспроводные сети имеют ряд ограничений:

- меньшая, чем в проводных сетях, скорость;
- подверженность влиянию помех;
- более сложная схема обеспечения безопасности передаваемой информации.

[1] По аналогии с Hi-Fi.

На физическом уровне существует несколько вариантов спецификаций, которые отличаются используемым частотным диапазоном, методом кодирования и как следствие — скоростью передачи данных. Все варианты физического уровня работают с одним и тем же алгоритмом уровня MAC, но некоторые временные параметры уровня MAC зависят от используемого физического уровня.

4.3.2.1. Уровень доступа к среде стандарта 802.11

В сетях 802.11 уровень MAC обеспечивает два режима доступа к разделяемой среде:

- *распределённый режим (Distributed Coordination Function, DCF)*;
- *централизованный режим (Point Coordination Function, PCF)*.

Распределённый режим доступа DCF. В этом режиме реализуется *метод множественного доступа с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA)*. Вместо неэффективного в беспроводных сетях прямого распознавания коллизий по методу CSMA/CD здесь используется их косвенное выявление. Для этого каждый переданный кадр должен подтверждаться кадром положительной квитанции, посылаемым станцией назначения. Если по истечении оговорённого времени квитанция не поступает, станцияотправитель считает, что произошла коллизия.

Режим доступа DCF требует синхронизации станций. В спецификации 802.11 временны́е интервалы начинают отсчитываться от момента окончания передачи очередного кадра. Это не требует передачи каких-либо специальных синхронизирующих сигналов и не ограничивает величину пакета размером слота, так как слоты учитываются только при принятии решения о начале передачи кадра. Станция, которая хочет передать кадр, обязана предварительно прослушать среду.

Предусматривается два механизма обнаружения несущей: *физический* и *виртуальный*. Первый механизм реализован на физическом уровне и сводится к определению уровня сигнала в антенне и сравнению его с пороговой величиной. Виртуальный механизм обнаружения несущей основан на том, что в передаваемых кадрах данных, а также в управляющих кадрах ACK и RTS/CTS содержится информация о времени, необходимом для передачи пакета (или группы пакетов) и получения подтверждения. Все устройства сети получают информацию о текущей передаче и могут определить, сколько времени канал будет занят, т.е. устройство при установлении связи сообщает всем, на какое время оно резервирует канал. Как только станция фиксирует окончание передачи кадра, она обязана отсчитать интервал времени, равный межкадровому интервалу (IFS). Если после истечения IFS среда все ещё свободна, начинается отсчёт слотов фиксированной длительности. Кадр можно передавать только в начале какого-либо из слотов при условии, что среда свободна. Станция выбирает для передачи слот на основании усечённого экспо-

ненциального двоичного алгоритма отсрочки, аналогичного используемому в методе CSMA/CD. Номер слота выбирается как случайное целое число, равномерно распределённое в интервале [0, CW], где CW (Contention Window) — *конкурентное окно*.

Если же в начале какого-нибудь слота среда оказывается занятой, то вычитания единицы не происходит, и таймер «замораживается». В этом случае станция начинает новый цикл доступа к среде, изменяя только алгоритм выбора слота для передачи. Как и в предыдущем цикле, станция следит за средой и при её освобождении делает паузу в течение межкадрового интервала. Если среда осталась свободной, то станция использует значение «замороженного» таймера в качестве номера слота и выполняет описанную выше процедуру проверки свободных слотов с вычитанием единиц, начиная с замороженного значения таймера отсрочки.

Размер слота зависит от способа кодирования сигнала (например, для метода FHSS размер слота равен 28 мкс; для метода DSSS — 1 мкс). Размер слота выбирается таким образом, чтобы он превосходил время распространения сигнала между любыми двумя станциями сети плюс время, затрачиваемое станцией на распознавание занятости среды. Если такое условие соблюдается, то каждая станция сети сумеет правильно распознать начало передачи кадра при прослушивании слотов, предшествующих выбранному ею для передачи слоту. Это, в свою очередь, означает, что коллизия может иметь место только в том случае, когда несколько станций выбирают один и тот же слот для передачи. В этом случае кадры искажаются, и квитанции от станций назначения не приходят. Не получив в течение определённого времени квитанцию, отправители фиксируют факт коллизии и пытаются передать свои кадры снова. При каждой повторной неудачной попытке передачи кадра интервал [0, CW], из которого выбирается номер слота, удваивается. Если, например, начальный размер окна выбран равным 8 (т.е. CW = 7), то после первой коллизии размер окна должен быть равен 16 (CW = 15), после второй последовательной коллизии — 32 и т.д. Начальное значение CW, в соответствии со стандартом 802.11, должно выбираться в зависимости от типа физического уровня, используемого в беспроводной локальной сети.

Как и в методе CSMA/CD, в данном методе количество неудачных попыток передачи одного кадра ограничено, но стандарт 802.11 не устанавливает точного значения этого верхнего предела. Когда верхний предел в N попыток достигнут, кадр отбрасывается, а счётчик последовательных коллизий устанавливается в нуль. Этот счётчик также устанавливается в нуль, если кадр после некоторого количества неудачных попыток все же передаётся успешно.

В беспроводных сетях возможна ситуация, когда два устройства (A и B) удалены и не слышат друг друга, однако оба попадают в зону охвата третьего устройства C. Это так называемая *проблема скрытого терминала*. Если оба устройства A и B начнут передачу, то они принципиально не смогут обнаружить конфликтную ситуацию и определить, почему пакеты не проходят.

В режиме доступа DCF применяются меры для устранения эффекта скрытого терминала. Для этого станция, которая хочет захватить среду и в соот-

ветствии с описанным алгоритмом начинает передачу кадра в определённом слоте, вместо кадра данных сначала посылает станции назначения короткий служебный кадр RTS (Request To Send — запрос на передачу). На этот запрос станция назначения должна ответить служебным кадром CTS (Clear To Send — свободна для передачи), после чего станцияотправитель посылает кадр данных. Кадр CTS должен оповестить о захвате среды те станции, которые находятся вне зоны сигнала станцииотправителя, но в зоне досягаемости станцииполучателя, т.е. являются скрытыми терминалами для станцииотправителя.

Максимальная длина кадра данных 802.11 равна 2346 байт, длина RTS-кадра — 20 байт, CTS-кадра — 14 байт. Так как RTS- и CTS-кадры гораздо короче, чем кадр данных, потери данных в результате коллизии RTS- или CTS-кадров гораздо меньше, чем при коллизии кадров данных. Процедура обмена RTS- и CTS-кадрами не обязательна. От неё можно отказаться при небольшой нагрузке сети, поскольку в такой ситуации коллизии случаются редко.

Централизованный режим доступа PCF. Если в сети имеется точка доступа, то может применяться централизованный режим доступа PCF, обеспечивающий приоритетное обслуживание трафика. В этом случае точка доступа играет роль арбитра среды.

Режим доступа PCF в сетях 802.11 сосуществует с режимом DCF. Оба режима координируются с помощью трёх типов межкадровых интервалов.

После освобождения среды каждая станция отсчитывает время простоя среды, сравнивая его с тремя значениями:

- короткий межкадровый интервал (Short IFS, SIFS);
- межкадровый интервал режима PCF (PIFS);
- межкадровый интервал режима DCF (DIFS).

Захват среды с помощью распределённой процедуры DCF возможен только в том случае, когда среда свободна в течение времени, равного или большего, чем DIFS. То есть в качестве IFS в режиме DCF нужно использовать интервал DIFS — самый длительный период из трёх возможных, что даёт этому режиму самый низкий приоритет.

Межкадровый интервал SIFS имеет наименьшее значение, он служит для первоочередного захвата среды ответными CTS-кадрами или квитанциями, которые продолжают или завершают уже начавшуюся передачу кадра.

Значение межкадрового интервала PIFS больше, чем SIFS, но меньше, чем DIFS. Промежутком времени между завершением PIFS и DIFS пользуется арбитр среды. В этом промежутке он может передать специальный кадр, который говорит всем станциям, что начинается контролируемый период. Получив этот кадр, станции, которые хотели бы воспользоваться алгоритмом DCF для захвата среды, уже не могут этого сделать, они должны дожидаться окончания контролируемого периода. Его длительность объявляется в специальном кадре, но этот период может закончиться и раньше, если у станций нет чувствительного к задержкам трафика. В этом случае арбитр передаёт слу-

жебный кадр, после которого по истечении интервала DIFS начинает работать режим DCF.

На управляемом интервале реализуется централизованный метод доступа PCF. Арбитр выполняет процедуру опроса, чтобы по очереди предоставить каждой такой станции право на использование среды, направляя ей специальный кадр. Станция, получив такой кадр, может ответить другим кадром, который подтверждает приём специального кадра и одновременно передаёт данные (либо по адресу арбитра для транзитной передачи, либо непосредственно станции).

Для того чтобы какая-то доля среды всегда доставалась асинхронному трафику, длительность контролируемого периода ограничена. После его окончания арбитр передаёт соответствующий кадр, и начинается неконтролируемый период.

Каждая станция может работать в режиме PCF, для этого она должна подписаться на данную услугу при присоединении к сети.

4.3.2.2. Типы кадров MAC

Контрольные кадры. Способствуют надёжной доставке информационных кадров. Существует шесть подтипов контрольных кадров:

- *Опрос после выхода из экономичного режима (PS-опрос)*. Данный кадр передаётся любой станцией станции, включающей точку доступа. В кадре запрашивается передача кадра, прибывшего, когда станция находилась в режиме энергосбережения, и в данный момент размещённого в буфере точки доступа.
- *Запрос передачи (RTS)*. Данный кадр является первым из четвёрки, используемой для обеспечения надёжной передачи данных. Станция, пославшая это сообщение, предупреждает адресата и остальные станции, способные принять данное сообщение, о своей попытке передать адресату информационный кадр.
- *Готов к передаче (CTS)*. Второй кадр четырёхкадровой схемы. Передаётся станциейадресатом станцииисточнику и предоставляет право отправки информационного кадра.
- *Подтверждение (ACK)*. Подтверждение успешного приёма предыдущих данных, кадра управления или кадра PSопроса.
- *Без состязания (CFконец)*. Объявляет конец периода без состязания; часть стратегии использования распределённого режима доступа.
- *CFконец + CFподтверждение*. Подтверждает кадр CFконец. Данный кадр завершает период без состязания и освобождает станции от ограничений, связанных с этим периодом.

Информационные кадры. Существует восемь подтипов информационных кадров, собранных в две группы. Первые четыре подтипа определяют кадры, переносящие данные высших уровней от исходной станции к станции адресату.

- *Данные*. Просто информационный кадр. Может использоваться как в период состязания, так и в период без состязания.
- *Данные* + *CFподтверждение*. Может передаваться только в период без состязания. Помимо данных, в этом кадре имеется подтверждение полученной ранее информации.
- *Данные* + *CFопрос*. Используется точечным координатором для доставки данных к мобильной станции и для запроса у мобильной станции информационного кадра, который находится в её буфере.
- *Данные* + *CFподтверждение* + *CFопрос*. Объединяет в одном кадре функции двух описанных выше кадров.

Остальные четыре подтипа информационных кадров фактически не переносят данные пользователя.

- Информационный кадр *нулевая функция* не переносит ни данных, ни запросов, ни подтверждений. Он используется только для передачи точке доступа бита управления питанием в поле управления кадром, указывая, что станция перешла в режим работы с пониженным энергопотреблением.
- Оставшиеся три кадра (*CFподтверждение*, *CFопрос*, *CFподтверждение* + *CFопрос*) имеют те же функции, что и описанные выше подтипы кадров (*данные* + *CFподтверждение*, *данные* + *CFопрос*, *данные* + *CFподтверждение* + *CFопрос*), но не несут пользовательских данных.

Кадры управления. Кадры управления используются для управления связью станций и точек доступа.

- *Запрос ассоциации*. Посылается станцией к точке доступа с целью запроса ассоциации с данной сетью с *базовым набором услуг (Basic Service Set, BSS)*. Кадр включает информацию о возможностях, например, будет ли использоваться шифрование или способна ли станция отвечать при опросе.
- *Ответ на запрос ассоциации*. Возвращается точкой доступа и указывает, что запрос ассоциации принят.
- *Запрос повторной ассоциации*. Посылается станцией при переходе между BSS, когда требуется установить ассоциацию с точкой доступа в новом BSS. Использование повторной ассоциации, а не просто ассоциации, позволяет новой точке доступа договариваться со старой о передаче информационных кадров по новому адресу.
- *Ответ на запрос повторной ассоциации*. Возвращается точкой доступа и указывает, что запрос повторной ассоциации принят.
- *Пробный запрос*. Используется станцией для получения информации от другой станции или точки доступа. Кадр используется для локализации BSS стандарта IEEE 802.11.
- *Ответ на пробный запрос*. Отклик на пробный запрос.
- *Сигнальный кадр*. Передаётся периодически, позволяет мобильным станциям локализовать и идентифицировать BSS.
- *Объявление наличия трафика*. Посылается мобильной станцией с целью уведомления других (которые могут находиться в режиме пониженного

энергопотребления), что в буфере данной станции имеются кадры, адресованные другим.
- *Разрыв ассоциации*. Используется станцией для аннулирования ассоциации.
- *Аутентификация*. Для аутентификации станций используются множественные кадры.
- *Отмена аутентификации*. Передаётся для прекращения безопасного соединения.

4.3.2.3. Подстандарты

Стандарт IEEE 802.11b благодаря высокой скорости передачи данных, практически эквивалентной пропускной способности обычных проводных локальных сетей Ethernet, а также ориентации на диапазон 2,4 ГГц, 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, то стандартом 802.11b предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

Стандарт IEEE 802.11a имеет наибольшую ширину полосы пропускания 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, т.е. любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с.

При разработке стандарта 802.11g рассматривались две отчасти конкурирующие технологии: *метод ортогонального частотного разделения OFDM* и *метод двоичного пакетного свёрточного 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.

Набор стандартов 802.11 определяет целый ряд технологий реализации *физического уровня (Physical Layer Protocol, PHY)*:
- уровень PHY стандарта 802.11 со скачкообразной перестройкой частоты (FHSS) в диапазоне 2,4 ГГц;
- уровень PHY стандарта 802.11 с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц;

– уровень PHY стандарта 802.11b с комплементарным кодированием в диапазоне 2,4 ГГц;
– уровень PHY стандарта 802.11a с ортогональным частотным мультиплексированием (OFDM) в диапазоне 5 ГГц;
– расширенный физический уровень (Extended Rate Physical Layer, ERP) стандарта 802.11g в диапазоне 2,4 ГГц.

Каждый из физических уровней стандарта 802.11 имеет два подуровня:

– *процедуру определения состояния физического уровня* (Physical Layer Convergence Procedure, PLCP);
– *подуровень физического уровня, зависящий от среды передачи* (Physical Medium Dependent, PMD).

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 приёма данных через беспроводную среду. Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11.

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 счёт применения остальных составляющих физического уровня, остались бы нереализованными.

Скрэмблирование (перестановка элементов) — метод, посредством которого принимаемые данные делаются более похожими на случайные; достигается это путём перестановки битов последовательности таким образом, чтобы превратить её из структурированной в похожую на случайную. Дескрэмблер приёмника 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.

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

– передачу в диапазоне инфракрасных волн;
– технологию расширения спектра путём скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц;
– технологию 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). Область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: ненаправленную антенну, от-

ражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направленное излучение предназначено для организации двухточечной связи.

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. 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.

По сути, схема скачкообразной перестройки частоты обеспечивает медленный 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.

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 г., технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с.

IEEE 802.11b. 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.

Изначально стандарт IEEE 802.11 предусматривал работу в режиме DSSS с использованием так называемой Баркеровской последовательности (Barker) длиной 11 бит: B1 = (0b10110111000). Каждый информационный бит замещается своим произведением по модулю 2 (XOR) с данной последовательностью. В результате бит заменяется последовательностью 11 чипов. Далее сигнал кодируется посредством дифференциальной двух- или четырёхпозиционной 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 *CCK-модуляция*

(Complementary Code Keying — кодирование комплементарным кодом).

Стандарт IEEE 802.11a появился практически одновременно с IEEE 802.11b, в сентябре 1999 г. 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 передаётся 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. Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 — служебные.

IEEE 802.11g. Стандарт IEEE 802.11g по сути представляет собой перенесение схемы модуляции OFDM, 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. В качестве основного способа модуляции принята схема *CCK (Complementary Code Keying)*, а в качестве дополнительной возможности допускается модуляция PBSS.

Разработчики 802.11g предусмотрели CCK-модуляцию для скоростей вплоть 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, причём обмен будет происходить между устройствами 802.11g посредством OFDM, то оборудование 802.11b просто не поймёт, что другие устройства сети ведут передачу, и попытается начать трансляцию. Чтобы не допустить подобной ситуации, предусмотрена возможность работы в смешанном режиме — CCK-OFDM.

Одна из основных проблем 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 устройства 802.11g 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 ситу-

ации в 802.11 введён защитный механизм, предусматривающий перед началом информационного обмена передачу короткого кадра *запрос на передачу* (RTS) и получение кадра подтверждения *можно передавать* (CTS). Механизм RTS/CTS применим и к смешанным сетям 802.11b/g. Естественно, эти кадры должны транслироваться в режиме ССК, который обязаны понимать все устройства. Однако защитный механизм существенно снижает пропускную способность сети.

4.3.3. Технология Bluetooth

Bluetooth представляет собой беспроводную технологию, обеспечивающую беспроводную передачу данных на небольших расстояниях между различными устройствами (например, мобильными персональными компьютерами, мобильными телефонами и другими устройствами) в режиме реального времени. При этом возможна передача как цифровых данных, так и звуковых сигналов.

Работа над концепцией системы Bluetooth началась в 1994 г. шведской компанией Ericsson. В феврале 1998 г. по инициативе пяти ведущих зарубежных компаний — Ericsson, IBM, Intel, Nokia и Toshiba — была организована специальная группа (Special Interest Group, SIG) [4], в задачи которой входило продвижение этой технологии. В мае того же года последовало объявление об учреждении концерна Bluetooth. В конце 1999 г. появились первые спецификации на соответствующее оборудование, ставшие впоследствии стандартом де-факто. На спецификациях Bluetooth v. 1.x базируется стандарт IEEE 802.15.1 [5], утверждённый в 2002 г.

Устройства версий 1.0 и 1.0B имели плохую совместимость между продуктами различных производителей. Основным недостатком была невозможность реализовать анонимность на протокольном уровне.

В Bluetooth 1.1 было исправлено множество ошибок, найденных в 1.0B, добавлена поддержка для нешифрованных каналов, *индикация уровня мощности принимаемого сигнала (Received Signal Strength Indicator, RSSI)*.

В версии 1.2 (2003 г.) была добавлена *технология адаптивной перестройки рабочей частоты (Adaptive Frequency-Hopping Spread Spectrum, AFH)*, что улучшило сопротивляемость к электромагнитной интерференции (помехам) путём использования разнесённых частот в последовательности перестройки. Также увеличилась скорость передачи и добавилась технология *eSCO (Extended Synchronous Connections)*, которая улучшила качество передачи голоса путём повторения повреждённых пакетов. В *HCI (Host Controller Interface)* добавилась поддержка трёхпроводного интерфейса *UART (Universal Asynchronous Receiver/Transmitter)*.

Основные отличия Bluetooth 1.2: ускоренное установление соединения, адаптивная схема переключения каналов (от 20 до 79), усовершенствованные алгоритмы передачи данных.

Версия Bluetooth 2.0+EDR (2004 г.) состоит из двух частей, которые могут поддерживаться аппаратурой независимо: обновлённая версия специфи-

кации Bluetooth (без принципиальных отличий от версии 1.2) и *расширенный набор скоростей передачи данных (Enhanced Data Rate, EDR)*. В режиме EDR применяется дифференциальная фазовая модуляция, увеличивающая базовую скорость передачи с 1 до 3 Мбит/с.

Стандарт Bluetooth 2.0+EDR полностью совместим с Bluetooth 1.0 и 1.2; скорость передачи в пикосети не ограничивается скоростью самого медленного.

В 2007 г. появилась обновлённая версия Bluetooth 2.1 (полное название Bluetooth Core Specification Version 2.1 + EDR). Эта версия полностью совместима с версией 2.0. В ней удалось снизить энергопотребление, а также усовершенствовать алгоритм связи.

4.3.3.1. Основные параметры радиоинтерфейса Bluetooth

- Диапазон частот: 2,4–2,4835 ГГц — промышленный, научный и медицинский диапазон частот (Industrial, Scientific and Medical band, ISM band)[1].
- Число несущих частот: 23–79 с разносом 1 МГц (16/32 в одной пикосети).
- Метод доступа: скачкообразная перестройка частоты и *дуплексная передача с временны́м разделением каналов (Frequency-hopping spread spectrum / Time-Division Duplex, FHSS/TDD)* (1600 скачков в секунду).
- Метод модуляции: *частотная модуляция с гауссовским сглаживанием (Gaussian Frequency Shift Keying, GFSK)* — двухуровневая схема кодирования сигнала, в которой логическому 0 и 1 соответствуют две разные частоты, коэффициент сглаживания формы входных импульсов $h = 0,35$.
- Скорость передачи по радиоканалу: 1 Мбит/с.
- Полоса пропускания: 220 кГц (по уровню 3 дБ), 1 МГц (по уровню 20 дБ).
- Мощность передатчика: 100 мВт (для связи до 100 м; 20 дБм), 2 мВт (до 10 м; 4 дБм) и 1 мВт (10 см; 0 дБм).

4.3.3.2. Принцип работы

Абонентские устройства Bluetooth объединяются в группы (пикосети), совместно использующие один радиоканал. В состав каждой пикосети входят один ведущий приёмопередатчик (с опорным генератором, который синхронизирует внутренний трафик сети) и до семи ведомых (синхронизируемых). Ведомое устройство вычисляет разность между частотами собственного и ведущего генераторов, и в процессе вхождения в синхронизм эта погрешность учитывается, что обеспечивает точное соответствие излучаемой частоты данного и ведущего устройств.

Вид псевдослучайной последовательности однозначно идентифицирует ведущий приёмопередатчик, а её фаза (псевдослучайный сдвиг) является адресным признаком ведомого устройства. Период повторения последователь-

[1] ISM band определяет полосы частот (918, 2450 и 5800 МГц, 22,5 ГГц) для работы промышленной, научной и медицинской радиослужб.

ности, определяющей закон перестройки частоты, достаточно большой (свыше 23 ч.). В каждой пикосети используется своя псевдослучайная последовательность, что позволяет множеству пикосетей одновременно работать по одному и тому же каналу связи, не создавая взаимных помех.

4.3.3.3. Синхронное и асинхронное соединения

Bluetooth имеет возможность организовывать как синхронное, так и асинхронное соединение.

Синхронное соединение (Synchronous Connection Oriented, SCO) возможно только в режиме точка–точка и применяется для передачи информации, чувствительной к задержкам (например, голоса). Основное (ведущее) устройство поддерживает до трёх синхронных соединений, подчинённое — до трёх синхронных соединений с одним основным устройством или до двух — с разными основными устройствами. При синхронном соединении основное устройство резервирует временны́е сегменты, следующие через так называемые SCO-интервалы. Даже если пакет принят с ошибкой, повторно при синхронном соединении он не передаётся.

Асинхронное соединение (Asynchronous Connection Less, ACL) возможно между основным и всеми активными подчинёнными устройствами в пикосети (режим точка–многоточка). Основное и подчинённое устройства могут поддерживать только одно асинхронное соединение. Подчинённое устройство отправляет пакет основному, только если в предыдущем временно́м интервале на его адрес пришёл пакет от основного устройства. Асинхронное соединение позволяет повторно передавать пакеты, принятые с ошибками.

Таким образом, Bluetooth может поддерживать один асинхронный канал данных (со скоростью до 723,2 Кбит/с в прямом и 57,6 Кбит/с в обратном направлениях), до трёх синхронных (с постоянной скоростью 64 Кбит/с в каждом направлении) голосовых каналов или канал с одновременной асинхронной передачей данных и синхронной передачей голоса (со скоростью до 433,9 Кбит/с в каждом направлении).

4.3.3.4. Структура кадра

Стандартный кадр Bluetooth содержит *код доступа (Access Code)* (длина 72 бита), *заголовок* (длина 54 бита) и *информационное поле* (длина не более 2745 бит) (рис. 4.1).

Рис. 4.1. Стандартный кадр Bluetooth

Код доступа идентифицирует пакеты, принадлежащие одной пикосети, а также используется для синхронизации и процедуры запросов; состоит из трёх полей:
- преамбулы (Preamble) (4 бита),
- кода синхронизации (Sync Word) (64 бита),
- концевика (Trailer) (4 бита контрольной суммы).

Заголовок (рис. 4.2) содержит информацию для управления связью и состоит из шести полей:
- поле *Адрес (AM_ADDR)* (3 бита) — содержит MAC-адрес узла назначения;
- поле *Тип пакета (TYPE)* (4 бита) — указывает код одного из 12 типов данных (ACL, SCO, опрос или пустой кадр), метод коррекции ошибок и число временны́х интервалов, из которых состоит кадр;
- поле *Поток (FLOW)* (1 бит) — осуществляет управление потоком данных, показывает готовность устройства к приёму;
- поле *Признак повторной передачи (ARQ)* (1 бит) — определяет корректность приёма;
- поле *SEQN* (1 бит) — служит для определения последовательности пакетов;
- поле *Контроль ошибок в заголовке (Header Error Check, HEC)* (8 бит) — контрольная сумма.

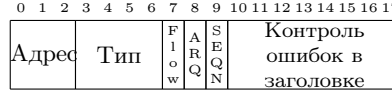

Рис. 4.2. Заголовок Bluetooth

Информационное поле имеет три сегмента:
- поле *Заголовок полезной информации* (8 бит) определяет логический канал, управление потоком в логических каналах, а также имеет указатель длины полезной информации;
- поле *Тело полезной информации* (0–2721 бит) включает пользовательскую информацию; длина этого сегмента указана в поле длины заголовка полезной информации;
- поле *Циклический избыточный код (Cyclic Redundancy Check, CRC)* (16 бит) служит для контроля целостности передаваемых данных.

Существует шесть типов пакетов Bluetooth.

4.3.3.5. Протоколы Bluetooth

Иерархия протоколов Bluetooth не соответствует моделям ISO/OSI, TCP/IP и IEEE 802. В спецификации определено 5 уровней: физический, базовый, управления каналом, сетевой и уровень приложений.

На *физическом уровне* определены параметры радиоинтерфейса Bluetooth.

Базовый уровень (baseband) и *уровень управления связью (Link Control Layer)* обеспечивают физическую радиочастотную связь между устройствами Bluetooth, образующими пикосеть.

На базовом уровне определено 13 типов пакетов. Пакеты ID, NULL, POLL, FHS , DM1 определены как для синхронных, так и для асинхронных соединений. Пакеты DH1, AUX1, DM3, DH3, DM5 и DH5 определены только для асинхронного соединения. Форматы пакетов HV1, HV2, HV3 и DV определены только для синхронного соединения. Кроме того, на данном уровне определены пять логических каналов: *LC (Control Channel)* и *LM (Link Manager)* используются на канальном уровне, а *UA (User Asynchronous)*, *UI (User Isosynchronous)* и *US (User Synchronous)* служат для асинхронной, изосинхронной и синхронной транспортировки пользовательских данных.

Протокол управления связью (Link Manager Protocol, LMP) отвечает за установление подключений между устройствами Bluetooth. Также сюда относятся и вопросы безопасности, такие как идентификация и шифрование, связанные с генерированием ключей шифрования и подключения, а также с обменом ключами и их проверкой. Кроме того, протокол контролирует режимы питания и исполнительные циклы устройств Bluetooth, а также состояние подключения того или иного устройства к пикосети.

Протокол управления логическим подключением и адаптацией (Logical Link Control and Adaptation Protocol, L2CAP) адаптирует протоколы верхнего уровня над Baseband. L2CAP является базовым протоколом передачи данных для Bluetooth. L2CAP работает только с ACLсоединениями. Многие протоколы и службы более высокого уровня используют L2CAP как транспортный протокол.

Протокол обнаружения услуг (Service Discovery Protocol, SDP) использует L2CAP в качестве транспортного протокола, что позволяет запросить информацию о самом устройстве, его услугах и характеристиках этих услуг, а после этого может быть установлено соединение между двумя или несколькими устройствами Bluetooth.

Протокол замены кабеля (RFCOMM) также использует L2CAP в качестве транспортного протокола. Протокол RFCOMM эмулирует соединение PPP (point-to-point) по последовательному порту, обеспечивает транспортировку при выполнении услуг верхнего уровня.

Двоичный протокол управления телефонией (Telephony Control Protocol Specification Binary, TCS Binary) является биториентированным протоколом и определяет контроль сигнализации вызова для установления речевого вызова или вызова данных между устройствами Bluetooth. Кроме того, он определяет процедуры управления мобильностью при манипулировании с группами TCS-устройств Bluetooth.

4.3.3.6. Профили Bluetooth

Профили Bluetooth представляют собой общие механизмы (протоколы и функции), через которые доступные устройства Bluetooth взаимодействуют

с другими устройствами. Профили определяют области возможного применения устройства Bluetooth. Если устройства от различных производителей соответствуют одному профилю, определённому в спецификации Bluetooth, они смогут взаимодействовать друг с другом.

- *Профиль общего доступа (Generic Access Profile, GAP)*
  Профиль GAP отвечает за поддержание связи между устройствами, выявление других доступных профилей, а также за безопасность соединений. Этот профиль должен быть включён во все устройства Bluetooth. В него входят функции, необходимые для работы всех основных протоколов Bluetooth.
- *Профиль последовательного порта (Serial Port Profile, SPP)*
  Профиль SPP позволяет устройствам Bluetooth эмулировать последовательный порт при помощи протокола RFCOMM. Профиль SPP определяет, каким образом два доступных устройства Bluetooth будут осуществлять обмен данными посредством эмуляции интерфейса RS-232 или интерфейса USB.
- *Профиль приложения обнаружения услуг (Service Discovery Application Profile, SDAP)*
  Профиль SDAP описывает, каким образом приложение должно использовать *протокол обнаружения услуг (Service Discovery Protocol, SDP)*. Профиль SDAP необходим для того, чтобы любое приложение имело возможность узнать, какие услуги (сервисы) Bluetooth является доступными на любом устройстве Bluetooth, с которым оно соединено.
- *Общий профиль обмена объектами (Generic Object Exchange Profile, GOEP)*
  Профиль GOEP используется для непосредственного (без использования IP) обмена объектами между двумя устройствами. Объект может иметь любой тип, например, изображение, документ, визитная карточка и т.д. Профиль определяет устройству одну из двух ролей: сервер, который определяет место, куда объект был помещён, и клиент, который инициализирует механизм передачи.
- *Профиль дозвона по сети (Dial-Up Networking Profile, DUN)*
  DUN обеспечивает стандартный доступ к сети Интернет и другому сервису модемной связи по беспроводной технологии Bluetooth.
- *Профиль факсимильной связи (Fax Profile, FAX)*
  Профиль FAX определяет, каким образом устройство, имеющее шлюз факсимильного аппарата, может использоваться в качестве оконечного устройства. Профиль FAX предназначен для обеспечения интерфейса между мобильным телефоном (или телефоном стационарной сети) и персональным компьютером с установленным программным обеспечением, поддерживающим факс.
- *Профиль гарнитуры (Headset Profile, HSP)*
  Профиль HSP определяет способ, посредством которого Bluetooth обеспечивает беспроводное соединение устройства с гарнитурой, оснащённой динамиками и, возможно, микрофоном.
- *Профиль доступа к локальной сети (LAN Access Profile, LAP)*

Профиль LAP предназначен для создания IP-сетей и позволяет создавать небольшие беспроводные сети Intranet, объединяющие ПК или смартфоны. Он также используется точками доступа для связи с кабельными сетями, будь то локальные сети или Internet.

– *Профиль передачи файлов (File Transfer Profile, FTP)*
Профиль FTP определяет, каким образом файлы на устройстве сервера могут быть просмотрены устройством клиента. Если местонахождение файла определено клиентом, то файл может быть перемещён от сервера к клиенту или помещён клиентом на сервер, используя профиль GOEP.
– *Профиль помещения объектов в стек (Open Push Profile, OPP)*
Профиль OPP управляет обменом электронными визитками в формате vCard (расширение файлов *.vcf). Эти визитки содержат ту же информацию, что и традиционные, но при этом они могут быть автоматически занесены в личную информационную систему (PIM) или в базу данных.
– *Профиль синхронизации (Synchronization Profile, SYNC)*
Профиль SYNC используется вместе с GOEP, чтобы обеспечить синхронизацию календаря и адресной информации (элементы управления персональной информации — PIM) между доступными Bluetoothустройствами. Основное применение этого профиля — обмен данными между персональным цифровым секретарём (PDA) и компьютером.
– *Профиль беспроводной телефонной связи (Cordless Telephony Profile, CTP)*
Профиль CTP определяет, каким образом беспроводной телефон может быть использован в технологии Bluetooth. Этот профиль может использоваться или для беспроводного телефона, или для мобильного телефона, который функционирует как беспроводной телефон вблизи от базовой станции.
– *Профиль внутренней связи (Intercom Profile, ICP)*
Этот профиль обеспечивает двустороннюю голосовую связь между устройствами Bluetooth. Он рассчитан на прямое взаимодействие двух устройств, расположенных в зоне взаимной досягаемости. Технология была разработана таким образом, чтобы, с одной стороны, не создавать ненужных помех для других пользователей, а с другой — быть невосприимчивым к радиосигналам других технологий, работающих на этих же частотах.

Дополнительные профили Bluetooth для устройств печати:

– *Профиль замены кабеля твёрдой копии (Hard Copy Cable Replacement Profile, HCRP)*
Профиль HCRP обеспечивает беспроводной вариант связи в качестве замены кабельного соединения между устройством и принтером.
– *Основной профиль принтера (Basic Printing Profile, BPP)*
Профиль BPP обеспечивает механизм формирования заданий вывода на печать текстов, сообщений электронной почты, изображений, визиток типа vCards и других объектов. Отличие этого профиля от HCRP заключается в том, что BPP не требует наличия специфических драйверов для каждого конкретного принтера.

Дополнительные профили Bluetooth для аудио- и видеоаппаратуры:

– *Общий профиль распространения аудио и видео (General Audio/Video Distribution Profile, GAVDP)*
  Профиль GAVDP является основой для профилей A2DP и VDP, применяемых в системах распределения видео- и аудиопотоков, использующих беспроводную технологию Bluetooth.
– *Расширенный профиль распространения аудио (Advanced Audio Distribution Profile, A2DP)*
  Профиль A2DP описывает, каким образом качественный стереозвук проходит от источника до приёмника.
– *Профиль распространения видео (Video Distribution Profile, VDP)*
  Профиль VDP определяет, каким образом доступное Bluetoothустройство обеспечивает передачу потоков видеоинформации, используя Bluetooth-технологии.
– *Профиль дистанционного управления аудио- и видеоаппаратурой (Audio/Video Remote Control Profile, AVRCP)*
  Профиль AVRCP обеспечивает стандартный интерфейс для управления высококачественной аудио- и видеоаппаратурой. Использование этого профиля позволяет единственному пульту дистанционного управления осуществлять управление всей аудио- и видеоаппаратурой, которая находится в окрестности. Профиль AVRCP даёт возможность управлять характеристиками мультимедиа потоков, например, регулировкой громкости, пуском, приостановкой и остановкой плейера, а также выполнять другие подобные операции дистанционного управления.

Основную конфигурацию дополняют другие профили Bluetooth:

– *Основной профиль изображения (Basic Imaging Profile, BIP)*
  Профиль BIP обеспечивает механизм дистанционного управления устройствами записи, передачи и отображения изображений (например, управление затвором цифровой фотокамеры с помощью мобильного телефона). Добавляется в основную конфигурацию профилей под управление профиля GOEP.
– *Профиль Hands-Free (Hands-Free Profile, HFP)*
  Профиль HFP описывает, каким образом устройствошлюз может использоваться для размещения и получения вызовов устройства hands-free. Типичный пример — применение мобильного телефона в качестве устройствашлюза. Профиль HFP позволяет также использовать ресурсы мультимедиа персонального компьютера в качестве аппаратуры громкой связи мобильного телефона. Добавляется в основную конфигурацию профилей под управление профиля SPP.

Глава 5. Сетевой уровень

5.1. Коммутация пакетов по меткам (MPLS)

Технология коммутации пакетов по меткам в многопротокольных сетях (Multiprotocol Label Switching, MPLS) представляет собой механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов (RFC 3031 [6]).

В традиционной IP-сети при передаче пакетов маршрутизаторы на основе данных заголовков (адрес назначения) принимают решение о выборе дальнейшего маршрута.

В сетях на базе протокола MPLS заголовки передаваемых пакетов не анализируются при прохождении через маршрутизаторы, а переадресация осуществляется исключительно на основе меток.

5.1.1. Архитектура MPLS

В основе архитектуры MPLS, как следует из названия, лежит процесс коммутации пакетов по меткам. *Метка (Label)* представляет собой короткий идентификатор фиксированной длины, который определяет принадлежность пакета к некоторому классу на каждом из участков коммутируемого маршрута.

Сеть MPLS делится на две области — *ядро* и *граничную область* (рис. 5.1).

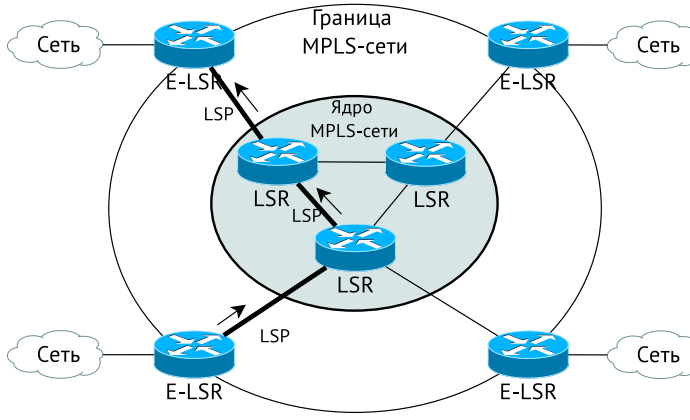

Рис. 5.1. Архитектура сети MPLS

Ядро образуют устройства *Label-Switch Routers (LSR)* — маршрутизаторы, поддерживающие как обычную IP-маршрутизацию, так и коммутацию по меткам. Маршрутизаторы ядра отвечают только за коммутацию. Границу сети MPLS образуют *граничные маршрутизаторы (Edge LSR, E-LSR)*, осуществляющие классификацию поступающих в MPLS-сеть пакетов, их фильтрацию, управление трафиком и т.п. Первая метка, устанавливаемая на граничном маршрутизаторе, определяет *маршрут следования (Label Switch Path, LSP)* пакета через MPLS-домен.

Множество подсетей, поставленное в соответствие конкретному LSP, образуют *класс эквивалентности (Forwarding Equivalence Classes, FEC)*. Каждый из классов FEC обрабатывается отдельно — строится свой путь LSP, выделяется своя ширина полосы пропускания канала и т.п.

LSR выполняет две функции — *маршрутизацию* и *коммутацию по меткам*.

Процесс маршрутизации функционирует на базе внутреннего протокола маршрутизации (например, OSPF). LSR получает маршрутную информацию от соседних маршрутизаторов и формирует таблицу маршрутизации, которая используется для маршрутизации IP-пакетов.

Процесс коммутации функционирует на базе *протокола обмена метками (Label Distribution Protocol, LDP)*, ставящего в соответствие конкретному значению метки определённый маршрут LSP.

5.1.2. Формат MPLS-метки

На рис. 5.2 представлен формат MPLS-метки (RFC 3032 [7]).

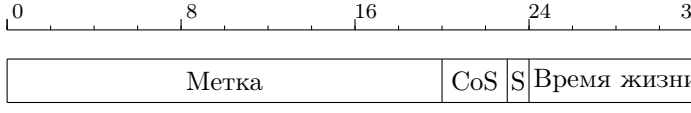

Рис. 5.2. Формат MPLS-метки

Поле *Метка (Label)* (длина 20 бит) содержит код метки, по которой осуществляется коммутация.

Зарезервированные значения меток:

- 0 (IPv4 Explicit NULL Label) — указывает, что стек меток должен быть очищен, а переадресация пакета должна основываться на заголовке IPv4;
- 1 (Router Alert Label) — указывает на то, что переадресация пакета определяется меткой;
- 2 (IPv6 Explicit NULL Label) — указывает, что стек меток должен быть очищен, а переадресация пакета должна основываться на заголовке IPv6;
- 3 (Implicit NULL Label) — значение, присваиваемое маршрутизатором.

Поле *(Class of Service, CoS)* (длина 3 бита) характеризует класс обслуживания пакета.

Поле *S* может принимать значение 0 или 1, указывая, является ли метка последней в стеке меток, присвоенных одному пакету[1].

Поле *Время жизни (Time-to-Live, TTL)* (длина 8 бит) указывает в общем случае число возможных промежуточных узлов.

MPLS-метка передаётся в составе любого пакета, причём способ её присоединения к пакету зависит от используемой технологии канального уровня. MPLS-метка добавляется между заголовком кадра (второй уровень ISO/OSI) и заголовком пакета (третий уровень модели ISO/OSI) (рис. 5.3).

Рис. 5.3. Расположение MPLS-метки

5.1.3. Label Distribution Protocol

Протокол распространения меток (Label Distribution Protocol, LDP) предназначен для построения целостных маршрутов LSP (RFC 3036 [8]). LDP представляет собой набор процедур и сообщений, с помощью которых LSR формирует сетевой маршрут LSP путём установления соответствия между маршрутной информацией и каналами передачи данных.

В функции LDP входит: определение соседнего маршрутизатора, управление сессией, рассылка меток, уведомление об ошибках.

Обмены сообщениями LDP осуществляются путём посылки протокольных данных LDP (PDU) через LDP-секцию TCP-соединений. При этом каждый LDP PDU может содержать более одного LDP-сообщения. Каждый LDP PDU представляет собой LDP-заголовок (рис. 5.4), за которым следует одно или более LDP-сообщений.

Поле *Версия (Version)* (длина 2 байта) содержит код номера версии протокола.

Поле *Длина PDU (PDU Length)* (длина 2 байта) указывает общую длину PDU в октетах, исключая поля версии и длины PDU.

Поле *Идентификатор LDP (LDP Identifier)* (длина 6 байт) однозначно идентифицирует пространство меток LSR-отправителя. При этом первые четыре октета идентифицируют LSR и должны быть уникальными, а последние два октета идентифицируют пространство меток заданного LSR.

Все сообщения LDP имеют определённый формат (рис. 5.5).

Поле U представляет собой бит неизвестного сообщения; при $U = 1$ сообщение игнорируется.

[1] В рамках архитектуры MPLS вместе с пакетом разрешено передавать не одну метку, а целый стек.

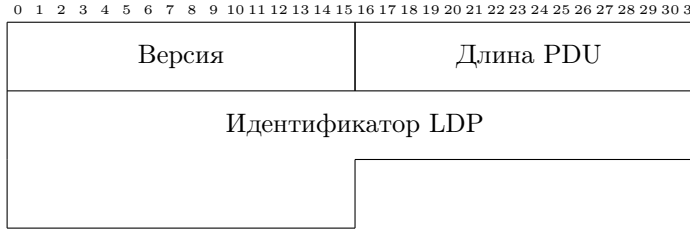

Рис. 5.4. Заголовок LDP

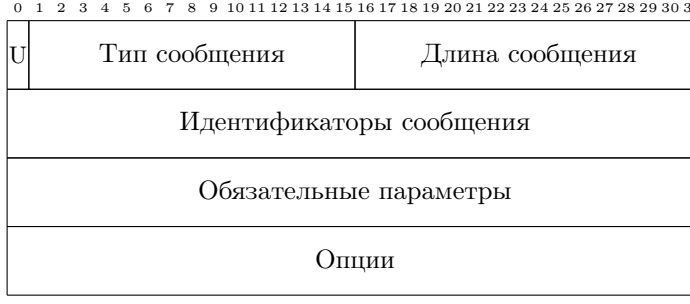

Рис. 5.5. Формат LDP-сообщений

Поле *Тип сообщения (Message Type)* идентифицирует тип сообщения.

Поле *Длина сообщения (Message Length)* указывает суммарную длину в октетах полей идентификатора сообщения, обязательных параметров и опций.

Поле *Идентификатор сообщения (Message ID)* идентифицирует сообщение.

Поле *Обязательные параметры* представляет собой набор необходимых параметров.

Поле *Опции* представляет собой набор необязательных параметров.

В LDP определены следующие типы сообщений:

- *Hello* — определение соседнего маршрутизатора;
- *инициализация (Init)* — процедура установления сессии;
- *KeepAlive* — используется для поддержания активного статуса LDP-сессии;
- *адрес (Address Message)* — анонсирование адреса интерфейса маршрутизатора;
- *отзыв адреса (Address Withdraw)* — отзыв ранее анонсированного адреса интерфейса;

- *присвоение метки (Label Mapping)* — сообщение о присвоении метки;
- *запрос метки (Label Request)* — запрос метки у соседнего маршрутизатора с целью установления соответствия значения метки и FEC;
- *запрос ликвидации метки (Label Release)* — подтверждение получения метки в сообщении Label Mapping;
- *отзыв метки (Label Abort Request)* — сигнал соседнему маршрутизатору о невозможности продолжения использования ассоциации FEC–метка;
- *освобождение метки (Label Withdraw)* — сообщение о ненужности ранее полученной метки.

Установление LDP сессии происходит по следующему сценарию:

- при помощи обмена сообщениями *Hello* соседние маршрутизаторы определяют транспортные адреса друг друга;
- один из маршрутизаторов становится активным;
- активный маршрутизатор устанавливает TCP/IP сессию на порт 646 и посылает сообщение *Init*, включающее в себя параметры LDP-сессии;
- пассивный маршрутизатор проверяет полученные параметры LDP-сессии на совместимость с локальными настройками LDP и посылает ответное сообщение *Init* со своими параметрами LDP-сессии;
- активный маршрутизатор также проверяет полученные параметры LDP-сессии на совместимость с локальными настройками LDP, после чего сессия считается установленной.

Если на каком-то этапе возникают ошибки, то сессия считается неустановленной, а маршрутизатор, обнаруживший ошибку, посылает сообщение *Shutdown* или *Reject* своему соседу.

LDP-сессия будет установлена, если совпадают версии протокола LDP и совпадают режимы распространения информации о метках.

5.1.4. Сервисы на базе MPLS

На базе MPLS возможна организация следующих сервисов:

- MPLS/VPN — создание распределённых виртуальных частных сетей (Virtual Private Network, VPN) на крупных сетях без организации туннелей и шифрования;
- MPLS/TrafficEnginering — гибкое управление потоками трафика внутри MPLS-домена и более полное использование канальной инфраструктуры сети;
- AnyTransportOverMPLS — прозрачная передача через MPLS-домен кадров ATM, Frame Relay, Ethernet и т.п.

5.1.5. Особенности MPLS

Главной особенностью MPLS является отделение процесса коммутации пакета от анализа IP-адресов в его заголовке. Вся информация о маршруте содержится в метке, и пакету не требуется нести адреса промежуточных узлов, что улучшает управление распределением нагрузки в сети.

В сетях MPLS есть возможность организации при помощи протокола RSVP явной коммутации пакетов через так называемые туннели, что повышает эффективность загрузки каналов в MPLS-сети с альтернативными путями, поскольку трафик с определённой меткой идёт по конкретному пути с заданными параметрами качества обслуживания. Такое решение снимает необходимость иметь маршрутную информацию на всех маршрутизаторах в сети оператора.

Ещё одной важной особенностью сетей MPLS является возможность разделения IP-трафика и создания VPN-соединений между различными узлами, а также независимость адресных пространств операторской и клиентских сетей. Такое решение даёт возможность масштабирования сети, интеграции сети с другими сервисами IP.

Глава 6. Транспортный уровень

6.1. Протокол SCTP

Протокол управления потоковой передачей (Stream Control Transmission Protocol, SCTP) (RFC 2960 [9], RFC 3286 [10]) можно рассматривать как дальнейшее логическое развитие протокола TCP. Как и TCP, протокол SCTP предлагает приложениям, взаимодействующим по IP-сети, ориентированную на соединения типа «точка-точка» транспортную службу с надёжной доставкой. Протокол унаследовал часть функциональности TCP, в том числе возможность контроля перегрузки и восстановления утерянных пакетов. Любое приложение, работающее по протоколу TCP, можно перевести на SCTP без потери функциональности.

6.1.1. Формат пакета SCTP

Сообщения SCTP включают общий заголовок, за которым следует один или несколько *подпакетов (Chunk)*, которые могут содержать данные или управляющую информацию (рис. 6.1). В заголовке (рис. 6.2) указываются номера портов отправителя и получателя, что позволяет мультиплексировать различные ассоциации SCTP на одном адресе.

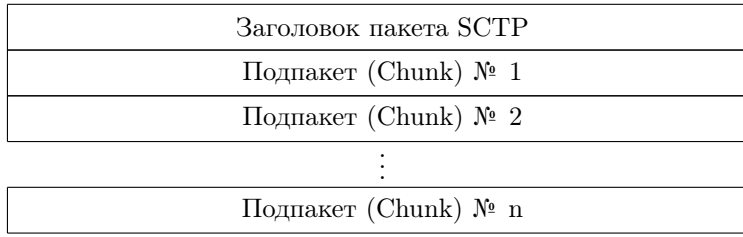

Рис. 6.1. Формат пакета SCTP

Проверочная метка (Verification Tag) (длина 32 бита) предотвращает возможность включения в ассоциацию SCTP устаревших или фальсифицированных сообщений.

Контрольная сумма (длина 32 бита) рассчитывается на основе полиномиального алгоритма CRC-32c и служит для выявления ошибок.

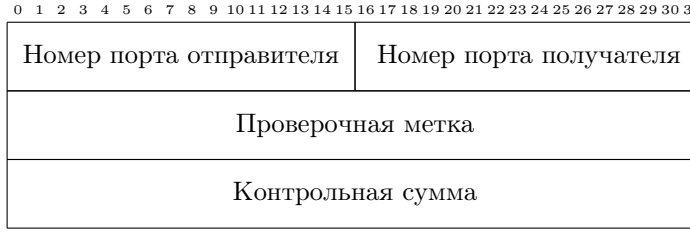

Рис. 6.2. Формат заголовка пакета SCTP

6.1.1.1. Формат подпакета

Каждый подпакет (фрагмент) содержит поля (рис. 6.3) *Тип подпакета (Chunk ID)*, *Флаги (Chunk Flags)*, *Длина подпакета (Chunk Length)*, *Данные (Chunk Value)*.

Рис. 6.3. Формат подпакета SCTP

Восьмибитное поле типа подпакета способно принимать до 255 значений (в настоящее время определены 15, а остальные зарезервированы). Если данное поле имеет нулевое значение, то это говорит о передаче *полезной информации (Payload Data)*; в других случаях подпакет несёт служебные сведения.

Второе поле — восьмибитное поле *флагов*, его использование определяется типом подпакета.

Поле *длины* с разрядностью 16 бит заполняется суммарным значением длины подпакета с учётом полей заголовка.

Управляющие блоки включают различные параметры и флаги, зависящие от типа блока. Подпакеты *данных (DATA)* включают флаг управления сегментацией и сборкой, а также параметры *TSN*, *Stream ID*, *Stream Sequence Number* и *Payload Protocol Identifier*.

Перед фрагментом DATA размещаются *номер транспортной последовательности (Transport Sequence Number, TSN)*, *идентификатор потока*, *номер последовательности потока (Stream Sequence Number, SSN)*.

Номер транспортной последовательности используется для обеспечения надёжности каждой ассоциации, а номер последовательности потока — для упорядочивания по потокам. Отдельные сообщения в потоке отмечаются идентификатором потока.

Информационная часть предназначена для передачи собственно данных, которые определяются типом подпакета. Согласно протоколу SCTP, размерность подпакета должна быть кратна 32 битам. В противном случае информационная часть дополняется нулевыми значениями, но в поле длины указывается истинная величина. Это позволяет на приёмной стороне соединения исключить добавленные нули из передаваемых данных.

Параметр *Payload Protocol ID* включён для обеспечения возможности расширения в новых версиях протокола. Если предположить, что функции идентификации протокола и мультиплексирования по портам в будущем перестанут играть столь важную роль, как сейчас, *Payload Protocol ID* будет обеспечивать идентификацию протоколов, передаваемых с помощью SCTP без использования номера порта.

Формат сообщений SCTP обеспечивает механизм связывания множества блоков данных и управления в одно сообщение для повышения эффективности транспорта. Использованием такой *группировки (Bundling)* управляет приложение, поэтому группировка стартовой передачи невозможна. Связывание естественным образом осуществляется при повторе передачи блоков *DATA* в целях снижения вероятности насыщения.

6.1.2. Функции SCTP

SCTP представляет собой unicast-протокол, который обеспечивает обмен данными между двумя конечными точками.

Аналогом TCP-соединения для SCTP является ассоциация, которая устанавливается между двумя оконечными устройствами. При этом одно устройство может быть определено несколькими IP-адресами, список которых передаётся при установлении ассоциации. Для передачи данных через ассоциацию используются все возможные комбинации адресов пары оконечных устройств.

Отказоустойчивость в таком случае обеспечивается за счёт того, что разные IP-адреса присваиваются различным интерфейсам устройств, и трафик между ними передаётся по разным маршрутам. В случае отказа какого-либо оборудования в сети и недоступности одного или нескольких IP-адресов трафик продолжает передаваться между оставшимися адресами, и разрыва SCTP-ассоциации не происходит.

Описанный выше механизм работы SCTP-ассоциации носит название *многодомности (SCTP Multi-Homing)*.

К другим ключевым функциям протокола SCTP относятся:

– группировка различных сигнальных сообщений в одном пакете с одним SCTP/IP-заголовком (Chunk Bundling), что повышает эффективность использования полосы пропускания;

- последовательная доставка сообщений внутри различных потоков, что позволяет избежать ситуации, встречающейся при использовании протокола TCP, когда в случае потери одного пакета остальные задерживаются в буфере до успешной его перепосылки (Head-of-Line Blocking);
- использование контрольных сумм для обеспечения безошибочной передачи пакетов, а также для защиты от атак.

Протокол SCTP поддерживает ряд функций, унаследованных не только от TCP, но и от других протоколов. При этом в нём реализованы и дополнительные функции:

- *Сохранение границ сообщений.* Сообщения, передаваемые SCTP, размещаются в подпакетах (или фрагментах), что даёт возможность приложениям отделить одно сообщение от другого.
- *Отсутствие блокировок типа head-of-line.* В отличие от TCP протокол SCTP не требует строгой упорядоченности передаваемых пакетов. Поэтому в нём отсутствует задержка, вызываемая блокировкой обслуживания, возникающей при восстановлении TCP корректной последовательности пакетов.
- *Несколько режимов доставки.* SCTP может передавать данные как в строгом порядке (как TCP), так и частично упорядоченные (по потокам) и неупорядоченные вовсе (как UDP).
- *Поддержка многодомности.* SCTP может переадресовывать пакеты на альтернативный IP-адрес.
- *Контроль перегрузки*. SCTP использует стандартные методики, применяющиеся для контроля перегрузки в TCP, в том числе медленный старт, предотвращение перегрузки и быструю повторную передачу.
- *Выборочные подтверждения.* SCTP использует схему выборочного подтверждения, унаследованную из TCP, для восстановления утраченных пакетов.
- *Фрагментация пользовательских данных*. SCTP разбивает сообщения на фрагменты, чтобы *максимальный размер передаваемого элемента (Maximum Transfer Unit, MTU)* соответствовал ограничениям конкретного маршрута пересылки между взаимодействующими хостами (RFC 1191 [11]).
- *Механизм контроля работоспособности (Hearbeat).* SCTP посылает пакеты контроля работоспособности на адреса находящегося в режиме ожидания хоста, которые входят в ассоциацию. Протокол декларирует, что IP-адрес будет отключён, как только он достигнет порогового значения невозвращённых подтверждений о работоспособности.
- *Защита от DoS-атак.* SCTP использует механизм cookie при инициализации ассоциации, чтобы смягчить воздействие DoS-атак.

6.1.3. Множественность потоков и варианты доставки

Название протокола SCTP обусловлено его многопотоковой природой передачи данных. Поддержка множества одновременных потоков позволяет

распределить между этими потоками передаваемую информацию так, чтобы каждый из потоков обеспечивал независимую упорядоченную доставку данных. Потеря сообщения в любом из потоков оказывает влияние лишь на данный поток, не затрагивая работу других потоков данных.

Протокол TCP работает с одним потоком данных и обеспечивает сохранение порядка доставки байт из потока. Такой подход удобен для доставки файлов или записей, но он может приводить к дополнительным задержкам при потере информации в сети или нарушении порядка доставки пакетов. При возникновении подобных ситуаций протокол TCP должен дождаться доставки всех данных, требуемых для восстановления порядка.

В рамках одного соединения SCTP обеспечивает единый механизм управления потоком и контроля насыщения, что существенно снижает нагрузку на транспортный уровень.

SCTP разделяет понятия надёжной и упорядоченной доставки, в то время как в TCP эти два аспекта неразрывно связаны, так как все данные надёжно доставляются хосту-получателю и предоставляются приложению в той последовательности, в какой они передавались. Для этого TCP использует номер последовательности в заголовке каждого пакета.

Протокол SCTP поддерживает многопотоковую передачу за счёт устранения зависимости между передачей и доставкой данных. В частности, каждый блок полезной информации типа DATA (данные) использует два набора порядковых номеров. Номер TSN управляет передачей сообщений и детектированием их потери, а пара *идентификатор потока Stream ID–номер SSN* используется для управления порядком доставки потребителю полученных данных.

Такая независимость механизмов нумерации позволяет получателю незамедлительно обнаруживать пропуски данных, а также видеть влияние потерянных данных на поток. Утрата сообщения вызывает появление пропуска в порядковых номерах SSN для потока, на который это сообщение оказывает влияние и не вызывает такого пропуска для других потоков. Следовательно, получатель может продолжить доставку незатронутых потоков, не дожидаясь повтора передачи утраченного сообщения.

6.1.4. Многодомность

Механизм многодомности предназначен для повышения устойчивости сети к выходам из строя интерфейсов на хосте и ускорения восстановления в случае сбоя в сети. Но эффективность этого механизма падает, если путь взаимодействия внутри ассоциации проходит через единую точку сбоя сети.

Действующий вариант SCTP не поддерживает *распределения нагрузки (Load Sharing)*, поэтому многодомные хосты обеспечивают лишь избыточность соединений для повышения уровня надёжности. Один из адресов многодомного хоста указывается в качестве *основного (Primary)* и используется как адрес получателя для всех блоков данных при нормальной передаче. При передаче повторных блоков данных используется один из дополнительных

адресов с целью повышения вероятности доставки в конечную точку. При повторяющихся неоднократно повторах передачи принимается решение об отправке всех блоков данных с использованием альтернативного адреса, пока системе мониторинга не удастся увидеть доступность основного адреса.

Для поддержки множества интерфейсов конечные точки SCTP обмениваются списками своих адресов в процессе создания ассоциации. Каждая из конечных точек должна быть способна принимать сообщения с любого адреса, связанного с удалённым партнёром; на практике некоторые операционные системы могут использовать в пакетах циклический перебор адресов отправителя, и в таких случаях приём пакетов с различных адресов является нормальной ситуацией. Для всего списка адресов конечной точки в данной сессии используется один номер порта.

Для повышения уровня безопасности требуется, чтобы некоторые отклики передавались по адресу, указанному в поле отправителя сообщения, вызвавшего отклик. Например, когда сервер получает блок INIT от клиента для инициирования SCTP-ассоциации, сервер всегда будет передавать блок INIT ACK по адресу отправителя в заголовке IP-блока INIT.

6.1.5. Установление ассоциаций

SCTP, как и TCP, ориентирован на установление соединения. Оба протокола требуют определения состояния соединения на каждом хосте. Соединение TCP определяется двумя IP-адресами и двумя номерами портов. Ассоциация SCTP определяется как набор IP-адресов + порт на каждом хосте. Любые из IP-адресов на любом хосте могут указываться в качестве отправителя или получателя в IP-пакете и это корректно идентифицирует ассоциацию.

Перед началом обмена данными два SCTP-хоста должны передать друг другу информацию о состоянии соединений с помощью четырёхэтапной процедуры установки соединения (handshake) (рис. 6.4).

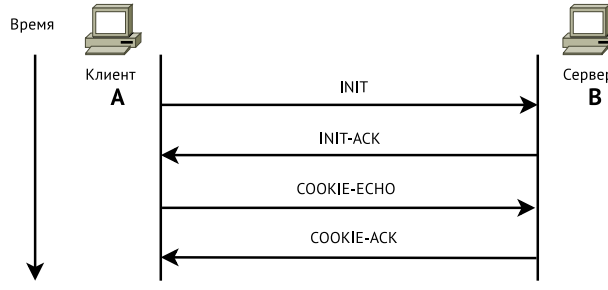

Рис. 6.4. Четырёхэтапная процедура установки соединения SCTP

Процедура, предусмотренная протоколом SCTP, позволяет защититься от

DoS-атак. Получателю сообщения о намерении установить контакт *INIT* в четырёхэтапной процедуре установки соединения не требуется сохранять никакую информацию о состоянии или резервировать какие-либо ресурсы. Вместо этого он посылает в ответ сообщение *INIT-ACK*, которое включает в себя *запись состояния (Cookie)*, содержащую всю информацию, необходимую отправителю *INIT-ACK* для того, чтобы сформировать своё состояние. Запись состояния подписывается цифровой подписью. Оба сообщения, *INIT* и *INIT-ACK*, содержат несколько параметров, необходимых для установки начального состояния:

- список всех IP-адресов, которые станут частью ассоциации;
- номер транспортной последовательности, используемый для надёжной передачи данных;
- тег инициации, который должен быть включён в каждый входящий пакет SCTP;
- число выходящих потоков, запрашиваемых каждой из сторон;
- число входящих потоков, которые способна поддерживать каждая из сторон.

После обмена этими сообщениями, отправитель INIT возвращает назад запись состояния в виде сообщения COOKIE-ECHO, которое также может содержать связанные с ним пользовательские сообщения DATA. При получении COOKIE-ECHO получатель полностью меняет своё состояние и отправляет обратное сообщение COOKIE-ACK, подтверждающее завершение настройки. COOKIE-ACK также может сопровождаться пользовательскими сообщениями DATA.

6.1.6. Завершение работы ассоциации

Транспортному протоколу, ориентированному на соединение, необходим метод постепенного отключения ассоциации. SCTP использует процедуру установки соединения, отличающуюся от процедуры, применяемой в TCP: конечная точка TCP может инициировать процедуру отключения, сохраняя открытым соединение и получая новые данные от другого хоста. SCTP не поддерживает такого наполовину закрытого состояния, т.е. обе стороны не могут передавать новые данные на свой более высокий уровень, если инициирована последовательность постепенного отключения.

Пусть приложение на хосте A хочет отключить и закрыть ассоциацию с хостом B. SCTP устанавливает состояние SHUTDOWN_PENDING, в котором он не будет принимать данные от приложения, но по-прежнему будет посылать новые данные, помещаемые в очередь на передачу на хост B. После подтверждения всех размещённых в очереди данных хост A посылает подпакет SHUTDOWN и устанавливает состояние SHUTDOWN_SENT.

До получения подпакета SHUTDOWN хост B уведомляет свой более высокий уровень, что прекращает принимать от него новые данные и вводит состояние SHUTDOWN_RECEIVED. Хост B передаёт оставшиеся данные на A, за которыми следуют фрагменты SHUTDOWN, информирующие B о по-

явлении данных и подтверждающие, что ассоциация отключена. Как только подтверждены все данные, помещённые в очередь на хосте B, хост A посылает соответствующий фрагмент SHUTDOWN-ACK, за которым следует фрагмент SHUTDOWN-COMPLETE, завершающий отключение ассоциации.

6.2. Протокол DCCP

Протокол DCCP (Datagram Congestion Control Protocol) [12, 13] является транспортным протоколом, который использует двунаправленные уникастные соединения с управлением перегрузкой для ненадёжной доставки дейтаграмм.

Протокол DCCP имеет встроенную систему управления перегрузкой, включающую поддержку *уведомления о перегрузке канала (Explicit Congestion Notification, ECN)* [14] для ненадёжных потоков дейтаграмм, исключая непредсказуемые задержки, характерные для TCP, что обеспечивает надёжное согласование параметров при установлении соединения.

6.2.1. Характеристики DCCP

Протокол DCCP обладает следующими характеристиками:
- является протоколом для потоков пакетов, а не потоков байт;
- реализует поток дейтаграмм с подтверждением получения, но без повторной посылки;
- имеет ненадёжный диалог установления и разрыва соединения;
- обеспечивает надёжное согласование параметров;
- предоставляет выбор механизмов подавления перегрузки;
- является протоколом управления перегрузкой, а не протоколом управления потоками;
- имеет опции, указывающие отправителю, был ли пакет доставлен получателю, помечен ECN, повреждён или отброшен входным буфером получателя;
- осуществляет управление перегрузкой со встроенной индикацией явной перегрузки ECN;
- обладает механизмами, позволяющими серверу избежать поддержки состояний неподтверждённых попыток соединений;
- выявляет MTU пути.

6.2.2. Типы сообщений DCCP

Протокол DCCP использует девять различных типов сообщений:
- DCCP-Request инициирует соединение;
- DCCP-Response является ответом на запрос DCCP-Request;
- DCCP-Data передаёт данные;
- DCCP-Ack передаёт подтверждения о получении пакетов;

– DCCP-DataAck передаёт данные в сочетании с подтверждениями;
– DCCP-CloseReq запрашивает закрытие соединения;
– DCCP-Close осуществляет закрытие соединения или запускает процедуру сброса соединения (DCCP-Reset);
– DCCP-Reset осуществляет процедуру сброса соединения;
– DCCP-Sync, DCCP-SyncAck осуществляют повторную синхронизацию номеров пакетов после длительного периода потерь.

6.2.3. Формат заголовка DCCP

Базовый заголовок DCCP имеет следующий формат (рис. 6.5).

Рис. 6.5. Формат базового заголовка DCCP

Поля *Порт отправителя (Source Port)* и *Порт получателя (Dest Port)* (длиной по 16 бит каждый) идентифицируют соединение. Когда соединение формируется, клиент должен выбрать порт отправителя случайным образом, чтобы уменьшить вероятность атаки.

Поле *Смещение данных (Data Offset)* (длина 8 бит) указывает смещение от начала заголовка пакета DCCP первого октета данных (выражается в 32-битных словах).

Поле *CCVal* (длина 4 бита) используется отправителем CCID.

Поле *Checksum Coverage* (CsCov) (длина 4 бита) определяет части пакета, которые покрываются полем *Контрольная сумма*.

Поле *Контрольная сумма (Checksum)* (длина 16 бит) содержит контрольную сумму заголовка пакета DCCP (включая опции), псевдозаголовка сетевого уровня и, в зависимости от CsCov, полей данных приложений.

Поле *Зарезервировано (Reserved)* (длина 3 бита) содержит нули, получатель должен это поле игнорировать.

Поле *Тип (Type)* (4 бита) специфицирует тип пакета.

Поле *Расширенные порядковые номера (X)* (длина 1 бит) равно нулю, если передаются только младшие (LSB) 24 бита порядкового номера, а базовый заголовок имеет длину 12 байт и значение 1, если в заголовке используются 48-разрядные порядковые номера. Пакеты DCCP-Data, DCCP-DataAck

и DCCP-Ack могут иметь значение, X равное 0 или 1. Все пакеты DCCP-Request, DCCPResponse, DCCP-CloseReq, DCCP-Close, DCCP-Reset, DCCP-Sync и DCCP-SyncAck должны иметь X=1.

Поле *Порядковый номер (Sequence Number)* (длина 48 или 24 бита) идентифицирует пакет в последовательности. Номер по порядку увеличивается на 1 после посылки каждого пакета, включая пакеты DCCP-Ack, которые не несут в себе данных.

После базового заголовка следует заголовок пересылаемого типа пакета.

6.2.4. Процедура взаимодействия

Процедура взаимодействия двух элементов следующая.

1. Клиент посылает серверу запрос DCCP-Request на установление соединения. Определяются номера портов клиента и сервера, запрашиваемая услуга и другие параметры соединения, включая CCID, необходимый серверу при работе с клиентом.
2. В ответ сервер посылает пакет-отклик.
3. Клиент посылает серверу подтверждение DCCP-Ack получения DCCPотклика.
4. Далее по необходимости происходит обмен подтверждениями DCCP-Ack для согласования используемых параметров.
5. Сервер и клиент обмениваются пакетами DCCP-Data, DCCP-Ack.
6. Для закрытия соединения сервер посылает DCCP-CloseReq.
7. Для подтверждения закрытия соединения клиент посылает DCCP-Close.
8. Сервер посылает пакет DCCP-Reset, при этом состояние соединения ликвидируется.
9. Клиент получает пакет DCCP-Reset и сохраняет своё состояние в течение некоторого времени для завершения происходящих обменов.

6.2.5. Функциональность DCCP

Протокол DCCP может реализовать механизм контроля за перегрузкой, многодомность и мобильность (за счёт механизма переадресации), процедуру медленного получателя (Slow Receiver). DCCP не предоставляет криптографических гарантий безопасности, но имеет возможности противостоять некоторым видам атак благодаря используемой системе нумерации пакетов.

Часть II

Мультисервисные сети

Глава 7. Понятие мультисервисных сетей

Мультисервисная сеть представляет собой инфраструктуру, использующую единый канал для передачи данных разных типов трафика.

Далее перечислены аспекты построения мультисервисных сетей:

- *конвергенция загрузки сети* — передача различных типов трафика в рамках единого формата представления данных;
- *конвергенция протоколов* — переход от множества существующих сетевых протоколов к общему;
- *физическая конвергенция* — передача различных типов трафика в рамках единой сетевой инфраструктуры;
- *конвергенция устройств* — построение архитектуры сетевых устройств, способной в рамках единой системы поддерживать разнотипный трафик;
- *конвергенция приложений* — интеграция различных функций в рамках единого программного средства;
- *конвергенция технологий* — создание единой общей технологической базы для построения сетей связи, способной удовлетворить требованиям и региональных сетей связи, и локальных вычислительных сетей;
- *организационная конвергенция* — централизация сетевых, телекоммуникационных, информационных служб под управлением менеджеров высшего звена.

Конвергирование подразумевает объединение двух направлений — коммутацию каналов (передачу голоса) и коммутацию пакетов (передачу данных). Поэтому далее сначала рассматривается мультисервисная сеть на базе коммутации каналов (ISDN), затем технологии для организации видеоконференций и других услуг по различным типам сетей передачи данных (H.323), сеть сигнализации № 7 как сеть управления мультисервисными сетями. Затем рассматриваются две концепции (Softswitch и IMS), имеющие возможность предоставления медиауслуг поверх различных сетей передачи. В заключение определяется понятие сетей следующего поколения (NGN), рассматриваются архитектура и концепции построения.

7.1. Концепция интеллектуальной сети

Интеллектуальная сеть (Intelligent Network, IN) представляет собой концепцию предоставления услуг связи, обладающих следующими характеристиками:

- модульность и многоцелевое назначение сетевых функций;
- интегрированные возможности разработки и внедрения услуг средствами модульных и многоцелевых сетевых функций;
- стандартизованное взаимодействие сетевых функций посредством независимых от услуг сетевых интерфейсов;

- возможность управления некоторыми атрибутами услуг со стороны абонентов и пользователей;
- стандартизованное управление логикой услуг.

Концепция интеллектуальной сети может быть применена к следующим типам сетей:

- телефонной сети общего пользования (Public Switched Telephone Network, PSTN);
- сети передачи данных с коммутацией пакетов (Data Packet Switched Network, DPSN);
- мобильной сети связи (Public Land Mobile Network, PLMN);
- узкополосной и широкополосной цифровой сети с интеграцией служб (Narrowband (Broadband) Integrated Services Digital Network, N(B)-ISDN).

7.1.1. Архитектура интеллектуальной сети

Архитектура интеллектуальной сети требует отделения функций предоставления услуг от функций коммутации, а также распределения этих функций по различным функциональным подсистемам. Таким образом, функции коммутации располагаются на уровне *базовой сети связи*, а функции предоставления услуг (управление, создание, внедрение) — на уровне *интеллектуальной надстройки*.

Взаимодействие между функциями этих уровней осуществляется посредством *прикладного протокола интеллектуальной сети (IN Application Protocol, INAP)*.Управление созданием и внедрением услуг осуществляется через *прикладной программный интерфейс (Application Programm Interface, API)*.

Концептуально архитектура интеллектуальной сети состоит из четырёх функциональных плоскостей:

- *плоскость услуг (Service Plane)* определяет набор услуг, предоставляемых интеллектуальной сетью пользователям сетей PSTN, ISDN и PLMN;
- *глобальная функциональная плоскость (Global Functional Plane, GFP)* описывает возможности сети, которые необходимы разработчикам для внедрения услуг;
- *распределённая функциональная плоскость (Distributed Functional Plane, DFP)* описывает функции, реализуемые узлами интеллектуальной сети;
- *физическая плоскость (Physical Plane, PP)* описывает узлы сети, содержащиеся в них функциональные элементы и протоколы взаимодействия.

Глобальная функциональная плоскость включает в себя следующие элементы:

- *независимые от услуг конструктивные блоки (SIB)* — обеспечивают выполнение стандартных многократно используемых сетевых функций;
- *точки инициации (POI)* — инициализируют обращения к блокам SIB;
- *точки завершения (POR)* — осуществляют воздействие на процесс обработки вызова, в результате чего обеспечивается услуга;

– *базовый процесс обработки вызовов (BCP)* — SIB, взаимодействующий с другими блоками посредством точек инициации и завершения.

7.1.2. Метод стандартизации концепции IN

Союз ITU-T разрабатывает долговременную архитектуру IN (Long Term IN Architecture), в основе которой лежит определение так называемых наборов возможностей CS (Capability Sets), описывающих конкретные аспекты целевой архитектуры IN. При спецификации очередного CS предполагается обратная связь с предыдущими этапами для внесения изменений в процесс эволюции IN. Разработка CS1 уже завершена в рамках рекомендаций серии Q.1200, определяющих функциональные возможности IN, основанных на существующих сетевых технологиях, например ISDN, и ориентированных на поддержку услуг, реализованных на базе сетей с коммутацией каналов. Отличительной особенностью данных услуг является то, что они могут быть активизированы только в процессе установления/разъединения соединения. По терминологии ITU-T услуги CS1 относятся к услугам типа A — являются одноконцевыми (Single Ended) с централизованной логикой управления (Single Point of Control).

ITU-T активно ведет работы по спецификации наборов CS2 и CS3 для широкополосных сетей, где также рассматриваются способы интеграции концепций IN с сетью управления телекоммуникациями TMN (Telecommunication Management Network).

7.1.3. Функции, реализуемые узлами интеллектуальной сети

Узлы интеллектуальной сети реализуют следующие функции:

– управление вызовом
  – *функция управления вызовом (Call Control Function)* обеспечивает возможности обслуживания вызовов;
  – *функция управления доступом вызова (Call Control Agent Function)* обеспечивает доступ пользователя в сеть;
  – *функция коммутации услуг (Service Switching Function)* обеспечивает интерфейс между функцией управления услугами и функцией управления вызовами;
  – *функция специализированных ресурсов (Specialized Resources Function)* обеспечивает доступ сетевых объектов к различным категориям сетевых средств (речевой автоинформатор, мосты конференц-связи и т.п.);
– управление услугами
  – *функция управления услугами (Service Control Function)* определяет логику услуг;
  – *функция поддержки данных услуг (Service Data Function)* управляет доступом услуг к базам данных сети и обеспечивает контроль данных;
– обеспечению услуг

- *функция среды создания услуг (Service Creation Environment Function)* специфицирует, создание, тестирование и загрузку программ логики услуг;
- *функция доступа к системе эксплуатационной поддержки и администрирования услуг (Service Management Access Function)* обеспечивает интерфейс к функции эксплуатационной поддержки и администрирования услуг;
- *функция эксплуатационной поддержки и администрирования услуг (Service Management Function)* обеспечивает предоставление услуг и административное управление ими.

7.1.4. Услуги интеллектуальной сети

Интеллектуальная сеть может предоставлять следующие услуги:

- *сокращённый набор (Abbrevated Dialing)* предоставляет пользователю возможность осуществления вызова, используя укороченный номер;
- *бесплатный вызов (Freephone)* предоставляет пользователю возможность не оплачивать разговор — оплату производит вызываемый абонент;
- *направленный вызов (Call forwarding)* позволяет направлять поступившие к пользователю вызовы на устройство с другим номером;
- телефонная конференция (Conferencing) позволяет нескольким абонентам принять участие в одном разговоре;
- *опрос населения (Mass Calling)* позволяет проводить опросы населения по телефону: абонент после вызова слышит объявление и просьбу набрать одну из нескольких цифр на телефоне, чтобы выразить своё предпочтение;
- *универсальный номер (Universal Access Number)* позволяет пользователю, имеющему несколько географически распределённых терминальных устройств, быть доступным другим пользователям по единому универсальному номеру в соответствии с определённой им маршрутизацией входящих вызовов;
- *виртуальная частная сеть (Virtual Private Network)* позволяет объединить часть имеющихся линий связи и коммутаторов в одну сеть, функционирование которой определяется пользователем (номера для пользователей этой сети, их права и приоритеты, маршрутизация вызовов и т.д.).

7.1.5. Концептуальная модель IN

7.1.5.1. Общие положения

Основой для стандартизации в области интеллектуальных сетей связи является абстрактная концептуальная модель — INCM, стандартизованная ITU-T в рекомендации I.312/Q.1201. Модель состоит из четырёх плоскостей, и отражает абстрактный подход к описанию IN.

Модель разделяет аспекты, относящиеся к услугам, и аспекты, связанные с сетью, что позволяет описывать услуги и возможности IN независимо от базовой сети над которой создается интеллектуальная надстройка.

Первый уровень — плоскость услуг (Service Plane) представляет взгляд на IN исключительно с точки зрения услуг. Здесь отсутствует информация о том, как именно осуществляется предоставление услуг сетью.

Второй уровень — глобальная функциональная плоскость GFP (Global Functional Plane) описывает возможности сети, которые необходимы разработчикам для внедрения услуг. Здесь сеть рассматривается как единое целое, даются модели обработки вызова (BCP) и независимых от услуг конструктивных блоков (SIB).

Третий уровень — распределенная функциональная плоскость DFP (Distributed Functional Plane) описывает функции, реализуемые узлами сети. Здесь сеть рассматривается как совокупность функциональных элементов, порождающих информационные потоки.

Четвертый уровень — физическая плоскость PP (Physical Plane) описывает узлы сети, содержащиеся в них функциональные элементы и протоколы взаимодействия.

7.1.5.2. Плоскость услуг

В рекомендациях ITU-T Q.1211 различают два термина *service* — услуга, и *service feature* — компонент услуги.

Услугой является самостоятельное коммерческое предложение, характеризуемое одним или более компонентами (возможностями), открытыми для дополнения. Компонент услуги является её специфической частью, который в совокупности с другими услугами и компонентами услуг может составлять часть самостоятельного коммерческого предложения, определяя составляющую, которая может быть различима пользователем.

Набор CS1 включает 25 видов услуг, которые должны поддерживаться сетями PSTN, ISDN и PLMN. Наиболее распространенные сегодня виды услуг представлены в таблице 2, где кроме англоязычного термина и аббревиатуры даются их значения и краткие пояснения.

Следует отметить, что определение набора услуг является одним из первых этапов при создании интеллектуальной сети в конкретном регионе и зависит от требований, сложившихся на местном рынке услуг связи.

7.1.5.3. Глобальная функциональная плоскость

Вторая плоскость модели (GFP) включает следующие основные элементы:

- базовый процесс обработки вызовов (BCP);
- независимые от услуг конструктивные блоки (SIB);
- точки инициации (POI) и точки завершения (POR).

Блоки SIB обеспечивают выполнение стандартных многократно используемых сетевых функций. Базовый процесс обработки вызовов является специализированным SIB, который взаимодействует с другими блоками посредством точек инициации и завершения. Если в процессе обработки вызова встретится одна из точек инициации, то это приводит к определенной последовательности обращений к блокам SIB. По завершении этой последовательности обращений осуществляется воздействие на процесс обработки вызова, зависящее от точки завершения. В результате такого взаимодействия может быть обеспечена услуга или компонент услуги. Таким образом, BCP описывает процесс обработки вызовов базовой сети связи из которой осуществляется запрос на услуги IN. Определенные на первом уровне INCM, услуги декомпозируются на компоненты и на плоскости GFP, объединяются в один или несколько SIB, которые при взаимодействии определяют глобальную логику услуги GSL (Global Service Lojic).

Выполняемые блоками SIB операции и данные, необходимые для их выполнения, специфицированы в рекомендации ITU-T Q.1213. Заметим, что Европейский институт стандартов электросвязи (ETSI) требует наличия в IN дополнительно еще семи блоков SIB.

7.1.5.4. Распределённая функциональная плоскость

На уровне третьем INCM (плоскость DPF) общесетевые функции определены в виде отдельных функциональных объектов (FE). Специфицированные на плоскости GFD блоки SIB реализуются на плоскости DFP в виде последовательности функциональных объектов (FEA), в результате выполнения которой возникают информационные потоки IF (Information Flows). В CS1 определено 60 различных IF, соответствующих процедурам прикладного протокола INAP.

Узлы IN, как правило, выполняют одну или несколько функций, которые делятся на три основные категории: функции, относящиеся к управлению вызовом, функции, относящиеся к управлению услугами и функции, обеспечивающие услуги (эксплуатационная поддержка и администрирование сети).

Функция коммутации услуг SSF тесно связана с функцией управления вызовом CCF. Обычно считается, что эти две функции образуют единый пакет SSF/CCF. Запрос на услугу как правило заключается в снятии трубки телефона и набору некоторого количества цифр. Роль функции коммутации услуг заключается в том, чтобы зафиксировать вызов и сформировать стандартный запрос. Функция управления вызовом не интеллектуальна, но запрограммирована так, чтобы распознать запрос на услугу и послать его функции управления услугами SCF.

Функция управления услугами SCF декодирует полученный запрос и интерпретирует его в контексте предоставляемых IN услуг. После этого формулируется, кодируется и посылается стандартное подтверждение, отсылаемое функции коммутации услуг SSF. Процесс формулирования подтверждения может включать выполнение комплекса программ, в том числе, контакт с вызываемым абонентом и обращение к функции поддержки данных SDF.

Функция коммутации услуг SSF, получив от SCF подтверждение, декодирует и интерпретирует его, а затем посылает функции управления вызовом CCF инструкции о том, как осуществить процесс установления соединением.

В процессе формулирования подтверждения от SCF к SSF может потребоваться диалог между SCF и вызывающим или вызываемым абонентом. Такой диалог обычно заключается в отправке подсказки и получении некоторой последовательности цифр. Функция управления услугами SCF не имеет средств для непосредственного осуществления такого диалога, который происходит не иначе, как с помощью функции специализированных ресурсов SRF. Обычно SCF обращается к SRF с запросом о соединении абонента с соответствующим устройством, входящим в SRF (например, с речевым автоинформатором), и о необходимости получить от абонента определенные данные.

Для понимания концепции интеллектуальной сети важно знать следующее:

1. Только функция управления вызовом CCF уполномочена контролировать процесс установления и разъединения соединения.
2. Взаимодействие функции коммутации услуг SSF и функции управления вызовом CCF является услуго-независимым. Поэтому SSF и CCF не должны содержать ничего, зависимого от услуг, предоставляемых IN.
3. В случае сбоев выполнения функции управления услугами SCF возможностей функций SSF/CCF должно быть достаточно для завершения вызова и соответствующего уведомления вызывающего и вызываемого абонентов.
4. Функция коммутации услуг SSF в любой момент времени не должна взаимодействовать более, чем с одной функцией управления услугами SCF.
5. Допускается взаимодействие между несколькими SCF и SSF но так, чтобы не нарушалось условие 4.
6. Только функция управления услугами SCF обладает всем необходимым для формулирования запросов к SRF, SSF и обработки ответов от них.
7. Не допускается какого-либо взаимодействия между SSF и SRF иначе, как через SCF.
8. Функция управления услугами SCF должна обладать возможностями для того, чтобы по инициативе вызываемого или вызывающего абонента приостановить предоставление услуги, но затем, в некоторый момент возобновить его по инициативе того же абонента.

В отличие от описанного порядка взаимодействия между SSF, SCF и SRF, который осуществляется по инициативе абонентов, функции, касающиеся обеспечения услуг инициируются операторами сети. Эти функции не связаны с каким-либо вызовом абонента или предоставлением конкретной услуги.

Функции SMF, SMAF и SCEF могут использоваться для удаления или изменения уже имеющихся услуг, а также для создания новых услуг. Это достигается путем изменения информации в SSF, SCF, SDF и SRF. Причем такие изменения не должны отражаться на качестве предоставляемых в этот момент услуг.

На четвертом уровне INCM определяются физические объекты (PE), способы отображения функциональных объектов на физические и описываются способы реализации сетевых элементов IN.

Основными требованиями к структуре IN являются:
- сетевые функции выполняются в узлах IN;
- в узле может выполняться одна или более функций;
- выполнение общей сетевой функции не может совместно осуществляться несколькими узлами;
- два различных узла могут выполнять одинаковые сетевые функции;
- узлы должны иметь стандартные интерфейсы;
- распределение сетевых функций по узлам и стандартные интерфейсы не должны зависеть от услуг, предоставляемых сетью.

Распределение сетевых функций по узлам IN может иметь следующий вид:

1. SSP (Service Switching Point): узел коммутации услуг. Кроме обеспечения пользователям доступа в сеть и выполнения любых необходимых для коммутации функций, SSP обеспечивает доступ к интеллектуальной сети. Он должен быть связан с узлами, выполняющими функции управления услугами (SCF), например, с узлами управления услугами SCP.
2. SCP (Service Control Point): узел управления услугами. Этот узел имеет набор программ, обеспечивающих выполнение услуг и, возможно, обработки данных, получаемых от пользователей IN. SCP выполняет функцию управления услуг SCF и, возможно, функцию поддержки данных SDF. SCP имеет прямой доступ к узлу поддержки данных SDP либо может подсоединяться к нему через сеть сигнализации. При этом узел SDP может входить как в ту же сеть, что и узел SCP, так и в другие сети. Через сеть сигнализации SCP может быть связан с узлом коммутации услуг SSP и интеллектуальной периферией (IP).
3. SDP (Service Data Point): узел поддержки данных. Данный узел содержит данные, необходимые для предоставления индивидуализированных услуг, т.е. выполняет функцию поддержки данных. Доступ к SDP может быть получен либо через сеть сигнализации, либо через узел управления услугами SCP или узел обеспечения услуг SMP. Различные узлы поддержки данных могут быть связаны друг с другом.
4. IP (Intelligent Peripheral): узел интеллектуальной периферии. Интеллектуальная периферия содержит средства, делающие услуги сети удобными для пользователей, например: запись речи пользователя, устройство распознавания речи, синтезатор речи. IP выполняет функции специализированных ресурсов SRF, функцию коммутации услуг SSF и функцию управления вызовом CCF. Последние две функции используются для обеспечения доступа к средствам, входящим в IP, который осуществляется по запросу из узла коммутации услуг SSP.
5. AD (Adjunct): вспомогательный узел управления. Данный узел аналогичен узлу управления услугами SCP, но имеет непосредственную связь с узлом коммутации услуг SSP. Связь между вспомогательным узлом управления и узлом коммутации услуг поддерживается по высокоскоростному каналу.
6. SN (Service Node): узел услуг. Данный узел напрямую связан с одним или более узлами коммутации услуг SSP и выполняет функции управления услугами SCF, поддержки данных SDF, специализированных ресур-

сов SRF, а также функции коммутации услуг SSF и управления вызовом CCF. При этом функции SSF/CCF в узле услуг тесно связаны с функцией управления услугами SCF и недоступны из других узлов, выполняющих функцию управления услугами. Данный узел имеет возможности как у узлов коммутации услуг, управления услуг и интеллектуальной периферии, вместе взятых.

7. SSCP (Service Switcing and Control Point): узел коммутации и управления услугами. Данный узел объединяет узлы коммутации и управления услугами и выполняет функции коммутации услуг SSF, управления вызовом CCF, управления услугами SCF, поддержки данных SDF, управлением доступа вызова CCAF и, возможно, функцию специализированных ресурсов SRF.
8. SMP (Service Management Point): узел обеспечения услуг. Данный узел выполняет функции SMF,SMAF и функцию среды создания услуг SCEF. Он может быть связан с любым узлом IN. Этот узел может управлять базами данных, тестировать сеть, управлять нагрузкой и проводить измерения различных характеристик сети.
9. SCEP (Service Creation Environment Point): узел среды создания услуг. Данный узел выполняет функцию среды создания услуг и служит для разработки, формирования, тестирования и внедрения услуг в пункте их обеспечения SMP.
10. SMAP (Service Management Access Point): узел доступа к системе эксплуатационной поддержки и администрирования услуг. Данный узел дает некоторым избранным пользователям доступ к узлам обеспечения услуг SMP.

Концептуальная модель представляет собой абстрактное средство для создания услуг IN путем их последовательного описания сверху вниз.

7.1.6. Архитектура прикладного протокола и интерфейсы IN

Концепция интеллектуальной сети при реализации ее сетевой архитектуры и прикладного протокола INAP использует один из ключевых элементов построения цифровых сетей связи - систему сигнализации SS7 (Signalling System № 7), стандартизованную ITU-T в рекомендациях серии Q.700. Дадим краткую характеристику SS7 в объеме, достаточном для определения прикладного протокола и интерфейсов IN.

7.1.6.1. Система сигнализации № 7

SS7 представляет собой стандартизованную на международном уровне общецелевую систему, предназначенную для осуществления обмена сигнальной информацией (информацией, передаваемой в процессе установления/разъединения соединений в сетях с цифровыми программно - управляемыми коммутационными станциями). Система оптимизирована для работы

по цифровым каналам со скоростью 64 Кбит/с и по сути является специализированной системой передачи данных с коммутацией пакетов переменной длины до 274 байт. Кроме процессов установления/разъединения соединений она используется для передачи данных между коммутационными станциями и специализированными узлами сетей связи. SS7 применяется на всех типах цифровых сетей - PSTN, N(B)-ISDN, PLMN, IN. Ее наличие на базовой сети является обязательным условием реализации IN и сетей сотовой подвижной связи в стандарте GSM.

7.1.6.2. Прикладной протокол IN

Архитектура прикладного протокола INAP определена в рекомендации ITU-T Q.1218, где рассматриваются два его основных варианта. Вариант А ориентирован на организацию множественных взаимнокоординируемых взаимодействий между прикладными процессами, а вариант В — на единичное взаимодействие прикладного процесса с другими процессами. Следует отметить, что в качестве основного интерфейса INAP ITU-T рекомендует подсистему TCAP SS7.

Более детальное описание INAP дано в рекомендации Q.1218 на языке ASN.1 (Abstract Syntax Notation One). Кроме того, в рекомендации Q.1218 определен набор возможных сценариев организации физических интерфейсов между различными типами структурных элементов ИС.

7.1.6.3. Интерфейсы IN

В рекомендации Q.1215 определен основной набор интерфейсов между физическими объектами IN.

Интефейсы SCP-SSP, SCP-IP и SCP-SDP осуществляются стеком протоколов SS7. Интерфейсы AD-SSP и AD-IP на верхнем уровне используют протокол TCAP SS7, а нижние уровни пока не специфицированы и здесь могут быть использованы протоколы аналогичные MTP и SCCP SS7 (например, X.25). В качестве интерфейсов IP-SSP и SN-SSP возможно применение базового метода доступа ISDN типа 2B+D. Пользователи используют существующие интерфейсы базовой, по отношению к IN, сети связи. Для сигнализации применяются либо стандартные аналоговые средства, либо сигнализация ISDN по D каналу.

7.2. Цифровая сеть с интеграцией служб (ISDN)

Цифровая сеть с интеграцией служб (Integrated Services Data Network, ISDN) представляет собой сеть с коммутацией каналов (телефонную сеть), обеспечивающую полностью цифровые соединения между оконечными устройствами для поддержания широкого спектра информационных услуг.

ISDN обеспечивает единый интерфейс доступа к цифровой сети передачи данных для устройств, выполняющих широкий набор задач, с сохранением

полной прозрачности сети для пользователей. Основное назначение ISDN — передача 64-Кбит/с по 4 КГц проводной линии и обеспечение интегрированных телекоммуникационных услуг.

7.2.1. Каналы ISDN

ISDN поддерживает три типа логических цифровых коммуникационных каналов, которые выполняют следующие функции:

B-канал используется для передачи информации (данные, видео и голос);

D-канал используется для передачи сигнализации и пакетов данных между пользовательским оборудованием и сетью;

H-канал выполняет те же самые функции, что и D-канал, однако работает при скорости, превышающей DS-0 (64 Кбит/с).

7.2.2. Устройства ISDN

В число компонентов ISDN входят:

- *терминальный адаптер (Terminal Adapter, TA)* — используется для подключения не-ISDN устройств к сети ISDN;
- *локальная станция (Local Exchange, LE)* — используется в телефонной станции, работает с протоколом ISDN и является частью сети;
- *локальное окончание (Local Termination, LT)* — используется для обозначения LE, служащих для работы с Local Loop (абонентским шлейфом);
- *оконечная станция (Exchange Termination, ET)* — используется для обозначения LE, отвечающих за функции коммутации;
- *сетевое оконечное оборудование (Network Termination, NT)*:
  - NT1 — служит для завершения соединений между пользователем и LE, отвечает за работу, мониторинг, подачу питания и мультиплексирование каналов;
  - NT2 — любое устройство, применяемое пользователем для коммутации, мультиплексирования и концентрации (локальная сеть, компьютер, терминальный контроллер и т. д.);
- *терминальное оборудование (Terminal Equipment, TE)* — любое пользовательское устройство (например, телефон или факсимильный аппарат).

7.2.3. Структура кадров ISDN

Кадры ISDN имеют следующую структуру (рис. 7.1).

Поле *Дискриминатор протокола* указывает протокол, используемый для оставшейся части.

Поле *Длина поля «Ссылка на вызов»* определяет длину следующего поля, которое может занимать один или два октета (в зависимости от типа используемого кодирования).

Поле *Флаг* имеет нулевое значение для сообщений, передаваемых стороной, выделяющей значения ссылки на вызов, 1 — в остальных случаях.

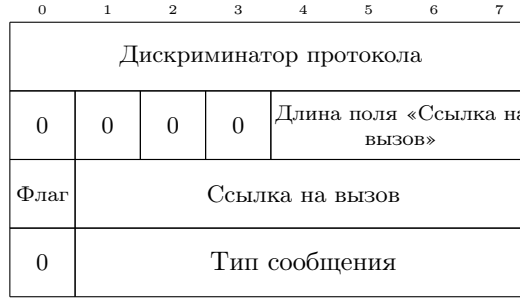

Рис. 7.1. Формат кадра ISDN

Поле *Ссылка на вызов* используется устройствами для идентификации соединения между устройством, инициировавшим вызов, и коммутатором ISDN.

Поле *Тип сообщения* определяет тип передаваемого сообщения и может занимать один или два (для специфических сообщений) октета. В двухоктетных сообщениях первый октет содержит восемь нулей.

7.2.4. Услуги сетей ISDN

Услуги идентификации номера:
- предоставление идентификации вызывающей линии;
- ограничение идентификации вызывающей линии;
- предоставление идентификации подключённой линии;
- ограничение идентификации подключённой линии;
- предоставление идентификации вызываемой линии;
- ограничение идентификации вызываемой линии;
- определение злонамеренного вызова;
- идентификация вызывающего при ожидании вызова.

Услуги, связанные с адресацией:
- прямой набор для УАТС;
- немедленный вызов к фиксированному адресату;
- задержанный вызов к фиксированному адресату;
- подадресация;
- преселекция;
- взаимодействующие номера;
- сокращённый адрес;
- несколько номеров у линии.

Услуги по завершению вызова:
- возврат вызова;
- ожидание вызова;

– завершение вызова по неответу;
– завершение вызова к занятому абоненту;
– перехват;
– услуга постановки в очередь.

Услуги переадресации:
– переадресация вызова безусловная;
– переадресация вызова при занятости;
– переадресация вызова по неответу;
– переадресация вызова на записанное сообщение;
– избирательная переадресация;
– передача вызова к звонку / к занято;
– отклонение вызова;
– ограниченная переадресация вызова.

Тарификация дополнительных услуг:
– информация о тарифе при установлении соединения;
– информация о тарифе в ходе разговора;
– информация о тарифе по завершении вызова;
– немедленный расчёт;
– бесплатный номер.

Услуги по ограничению:
– замкнутая группа пользователей;
– запрет входящего вызова;
– запрет исходящего вызова;
– не беспокоить;
– выборочный отказ от вызова;
– ограниченная передача вызова;
– приоритет;
– катастрофический приоритет;
– аварийная ситуация;
– редакция списка просмотра;
– выборочный приём вызова.

Услуги для нескольких участников:
– конференция с добавлением;
– конференция «Встреть меня»;
– трёхсторонняя конференция;
– удержание вызова;
– поиск линии.

Услуги мобильности:
– переносимость терминала;
– дистанционное управление;
– групповой поиск.

Специальные услуги предупреждений:
– вызов по тревоге;
– приоритетный вызов к охране.

Услуги, связанные с УАТС:
– прямой набор;

– общий и индивидуальный набор.

Управление дополнительными услугами:

– управление абонентами;
– удалённый доступ;
– общая пассивизация.

Дополнительные услуги:

– сигнализация от пользователя к пользователю;
– услуга передачи данных;
– подслушивание / перехват.

7.2.5. Технология Frame Relay

Frame Relay (FR) — ретрансляция кадров — технология доставки сообщений в сетях передачи данных с коммутацией пакетов.

В разработке стандартов Frame Relay приняли участие три организации:

– Frame Relay Forum (FRF) — международный консорциум, включающий в себя свыше 300 поставщиков оборудования и услуг, среди которых 3Com, Northern Telecom, Digital, Cisco, Netrix, Ascom Timeplex, Newbridge Networks, Zilog и др.;
– American National Standards Institute (ANSI) — Американский национальный институт по стандартизации;
– ITU-T (International Telecommunication Union) — Международный союз электросвязи.

В 1988 г. ITU-T (в то время CCITT) принял Рекомендацию I.122 «Обеспечение дополнительного пакетного режима», которая использовалась как часть серии стандартов ISDN. Комитет ANSI T1S1 занялся развитием положений I.122, завершившимся принятием стандартов, полностью определяющих Frame Relay. Стандарт T1.606 был одобрен в 1990 г., а остальные стандарты (T1.617, T1.618) приняты в 1991 г.

7.2.5.1. Принципы построения и компоненты сети Frame Relay

Физически сети Frame Relay образуют ячеистую структуру коммутаторов. Компоненты :

– *оконечное оборудование данных (Data Terminal Equipment, DTE)*;
– *оконечное оборудование каналов передачи данных (Data Circuitterminating Equipment, DCE)*;
– *FR-адаптеры и FR-интерфейсы (FR assembler/disassembler, FRAD)*.

Требования технологии Frame Relay:

– оконечные устройства должны поддерживать интеллектуальные протоколы более высоких уровней модели ISO/OSI;
– каналы связи должны быть свободны от ошибок;
– прикладные средства должны уметь осуществлять различные передачи.

7.2.5.2. Виртуальные каналы

Основу Frame Relay составляют *виртуальные каналы (Virtual Circuits)*. Виртуальный канал в сети Frame Relay представляет собой логическое соединение, которое создаётся между двумя устройствами DTE и используется для передачи данных.

В сети Frame Relay используется два типа виртуальных каналов — *коммутируемые (Switched Virtual Circuits, SVC)* и *постоянные (Permanent Virtual Circuits, PVC)*.

SVC устанавливается динамически. Для него стандарты передачи сигналов определяют, как узел должен устанавливать, поддерживать и сбрасывать соединение. Процесс передачи данных с использованием SVC состоит из четырёх последовательных фаз:

- *установление вызова (Call Setup)* — создаётся виртуальное соединение между двумя DTE;
- *передача данных (Data Transfer)* — фаза непосредственной передачи данных;
- *ожидание (Idle)* — виртуальное соединение ещё существует, но передача данных через него уже не производится; если период ожидания превысит установленное значение тайм-аута, соединение может быть завершено автоматически;
- *завершение вызова (Call Termination)* — фаза завершения соединения.

PVC включает в себя конечные станции, среду передачи и все коммутаторы, расположенные между конечными станциями. После установки PVC для него резервируется определённая часть полосы пропускания, и двум конечным станциям не требуется устанавливать или сбрасывать соединение.

Процесс передачи данных по каналу PVC имеет всего две фазы:

- передача данных — фаза непосредственной передачи данных;
- ожидание — виртуальное соединение существует, однако передача данных через него не производится.

В отличие от SVC, постоянный канал PVC не может быть автоматически разорван в том случае, если он не используется для передачи данных.

PVC имеют два преимущества над SVC:

- могут обеспечить более высокую производительность, так как соединение устанавливается предварительно и впоследствии не разрывается;
- обеспечивают лучший контроль над сетью, так как провайдер или сетевой администратор может выбирать путь, по которому будут передаваться кадры.

Однако и SVC имеют ряд преимуществ над PVC:

- могут имитировать сети без установления соединений (необходимо, если пользователь использует приложение, которое не может работать в сети с установлением соединения);
- используют полосу пропускания только тогда, когда это необходимо (PVC должны постоянно её резервировать на тот случай, если она понадобится);
- требуют меньшей административной работы, поскольку устанавливаются автоматически, а не вручную.

Однако режим SVC не получил широкого распространения, в силу сложности в реализации. Как следствие, PVC является наиболее распространённым режимом связи в сети FR.

7.2.5.3. Формат блока данных

На рис. 7.2 приведён формат кадра Frame Relay.

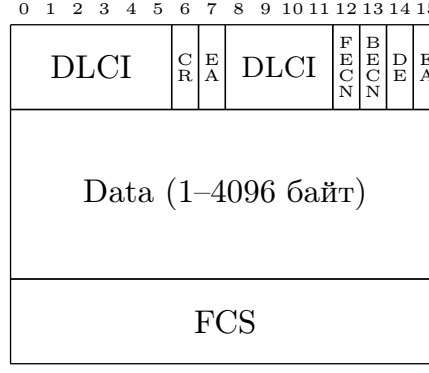

Рис. 7.2. Формат кадра Frame Relay

Поле *Флаг* обрамляет кадр Frame Relay.

Поле *Заголовок* содержит:

- поле *Идентификатор канала передачи данных (Data Link Connection Identifier, DLCI)* — определяет абонентский адрес в сети Frame Relay (стандарт FRF), состоит из шести бит первого октета и четырёх бит второго октета заголовка кадра (стандарты ANSI и ITU-T допускают размер заголовка до 4 байт);
- поле *Запрос/Ответ (Command/ Response, CR)* (2 бита) — зарезервировано для возможного применения в различных протоколах более высоких уровней модели ISO/OSI;
- бит *Расширение адреса (Extended Address, EA)* — устанавливается в конце каждого октета заголовка и указывает на наличие/отсутствие расширения заголовка Frame Relay на целое число дополнительных октетов с целью указания адреса, состоящего более чем из 10 бит, причём если бит имеет значение 1, то данный октет в заголовке последний;
- бит *Уведомление приёмника о явной перегрузке (Forward Explicit Congestion Notification, FECN)* — устанавливается аппаратурой канала данных в 1 для уведомления получателя сообщения о том, что произошла перегрузка в направлении передачи данного кадра;
- бит *Уведомление источника о явной перегрузке (Backward Explicit Congestion Notification, BECN)* — устанавливается аппаратурой канала

данных в 1 для уведомления источника сообщения о том, что произошла перегрузка в направлении, обратном направлению передачи содержащего этот бит кадра, после чего источник должен снизить интенсивность передаваемого потока данных;
- бит *Разрешения сброса (Discard Eligibility, DE)* — устанавливается в 1 (либо аппаратурой канала данных, либо оконечным оборудованием) в случае явной перегрузки и указывает на то, что данный кадр может быть уничтожен в первую очередь.

Информационное поле (Data) содержит данные пользователя и состоит из целого числа октетов. Его максимальный размер определён стандартом FRF и составляет 1600 байт (минимальный размер — 1 байт), но возможны и другие максимальные размеры (вплоть до 4096 байт). Содержание информационного поля пользователя передаётся без внесения изменений.

Поле *контрольная сумма (Frame Check Sequence, FCS)* (длина 2 байта) используется для обнаружения возможных ошибок при передаче. Содержит 16-разрядную контрольную сумму всех полей кадра Frame Relay, за исключением поля *Флаг*.

7.2.5.4. Адресация в сетях Frame Relay

Для идентификации виртуальных каналов в сети Frame Relay используется DLCI, который определяет номер виртуального порта для процесса пользователя. Обычно идентификатор DLCI имеет только локальное значение и не является уникальным в пределах сети. Конкретные значения DLCI для каждого пользователя определяются провайдером сервиса Frame Relay.

Дополнение в виде глобальной адресации позволяет применять идентификаторы узлов. При использовании этого дополнения значения, вставленные в поле DLCI блока данных, являются глобально значимыми адресами индивидуальных устройств конечного пользователя (например, маршрутизаторов). Аппаратура канала данных обязана обладать способностью определения принадлежности проходящего кадра конкретному PVC. Внутри сети Frame Relay могут использоваться различные сетевые адреса. Для разных интерфейсов одно и то же значение DLCI может применяться многократно.

7.2.5.5. Отличия протокола Frame Relay от HDLC

Отличия протокола Frame Relay от HDLC состоят в следующем:
- Frame Relay не предусматривает передачу управляющих сообщений;
- для передачи служебной информации используется специально выделенный канал сигнализации;
- отсутствует нумерация последовательно передаваемых (принимаемых) кадров, так как протокол Frame Relay не имеет никаких механизмов для подтверждения правильно принятых кадров.

7.2.5.6. Применение технологии Frame Relay

Данная технология применяется как для управления пульсирующим трафиком между локальными сетями и территориальной сетью, так и для передачи голоса.

7.2.5.7. Достоинства и недостатки

Достоинства:

- малое время задержки;
- простой формат кадров, содержащих минимум управляющей информации, следствием чего является высокая эффективность передачи данных (в предположении, что канал надёжен);
- независимость от протоколов верхних уровней модели ISO/OSI;
- предсказуемая пропускная способность;
- возможность контроля работоспособности (нагруженности) канала;
- возможность приоритезации разнородного трафика (для каждого типа трафика можно организовать своё виртуальное соединение).

Недостатки:

- Frame Relay не различает протоколы вышележащих уровней и, следовательно, нельзя приоритезировать трафик без организации дополнительных виртуальных соединений, что несёт дополнительные накладные расходы;
- отсутствие широковещательного множественного доступа;
- нет встроенных функций контроля доставки и управления потоком кадров (функции управления потоком выполняются протоколами верхних уровней).

7.3. Система сигнализации № 7

Система общеканальной сигнализации № 7 (ОКС7 — Signaling System № 7, SS7) обеспечивает связь между коммутационными станциями и специализированными узлами сетей связи.

Система применяется в следующих сетях связи:

- в телефонных сетях общего пользования (Public Switched Telephone Network, PSTN);
- в цифровых сетях с интеграцией служб (Integrated Services Digital Network, ISDN);
- в подвижных сетях (Public Land Mobile Network, PLMN),
- в сети сотовой подвижной связи стандарта GSM (Global System for Mobile communications);
- при реализации концепции интеллектуальной сети (Intelligent Network, IN).

7.3.1. Архитектура сети SS7

В сети SS7 определены следующие базовые функциональные элементы:

- *пункт сигнализации (Signaling Point, SP)* — любой узел сигнальной сети, реализующий функции обработки сигнальных сообщений SS7;
- *звено сигнализации (Signaling Link, SL)* — канал передачи данных, соединяющий между собой пункты сигнализации и состоящий из физического канала связи, терминального сигнального оборудования и протокола, контролирующего соединение;
- *транзитный пункт сигнализации (Signaling Transfer Point, STP)* — пункт сигнализации, осуществляющий только функции маршрутизации сигнальных сообщений между различными звеньями сигнализации и не имеющий подсистем пользователей.

Архитектура SS7 имеет модульную структуру, состоящую из нескольких функциональных блоков, причём в основе архитектуры лежит принцип разделения функций между *подсистемой передачи сообщений (Message Transfer Part, MTP)* и *подсистемами пользователей сигнальной сети (User Parts, UP)*. Подсистема передачи сообщений поддерживает не все необходимые функции маршрутизации и адресации сообщений, предусмотренные в модели ISO/OSI на сетевом уровне. Поэтому в SS7 введена подсистема управления сигнальным соединением (Signaling Connection Control Part, SCCP), предоставляющая расширенные услуги по адресации и передаче сообщений.

7.3.1.1. Подсистема MTP

Подсистема MTP обеспечивает корректную передачу информации между узлами сети сигнализации.

Подсистема состоит из следующих элементов:

- *звена передачи данных (MTP1)*;
- *функций управления звеном сигнализации (MTP2)*;
- *функций управления сетью сигнализации (MTP3)*.

MTP1 представляет собой полнодуплексное физическое соединение, состоящее из двух физических каналов, передающих информацию в противоположных направлениях с одинаковой скоростью.

MTP2 вместе с MTP1 образуют *звено сигнализации*, которое обеспечивает достоверную передачу сигнальных сообщений между двумя смежными пунктами сигнализации.

Базовыми элементами звена сигнализации являются *сигнальные единицы (Signal Unit)* — блоки данных переменной длины, в которых передаются любые другие сообщения SS7. Используется три типа сигнальных единиц:

- *значащие сигнальные единицы (Message Signal Unit, MSU)* — содержат данные подсистем пользователей или управляющую информацию MTP3;
- *сигнальные единицы состояния звена (Link Status Signal Unit, LSSU)* — содержат управляющую информацию уровня звена сигнализации;

– *заполняющие сигнальные единицы (Fill-In Signal Unit, FISU)* — генерируются звеном сигнализации, когда нет других сигнальных сообщений, и предназначены для контроля за работоспособностью звена сигнализации, так что дефектные звенья могут быть быстро обнаружены и отключены.

На рис. 7.3, 7.4, 7.5 приведены форматы сигнальных единиц MSU, LSSU, FISU.

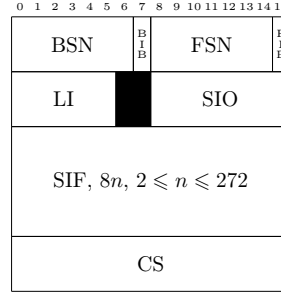

Рис. 7.3. Формат MSU

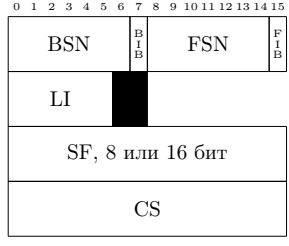

Рис. 7.4. Формат LSSU

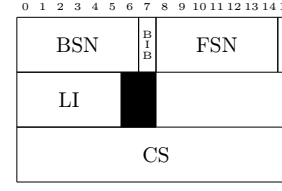

Рис. 7.5. Формат FISU

Все сигнальные единицы начинаются 8-битным полем *Флаг (Flag)*.

Поле *Обратный порядковый номер (Backward Sequence Number, BSN)* (длина 7 бит) содержит номер подтверждаемой сигнальной единицы.

Поле *Обратный бит-индикатор (Backward Indicator Bit, BIB)* (длина 1 бит) используется базовым методом коррекции ошибок.

Поле *Прямой порядковый номер (Forward Sequence Number, FSN)* (длина 7 бит) содержит номер передаваемой сигнальной единицы.

Поле *Прямой бит-индикатор (Forward Indicator Bit, FIB)* (длина 1 бит) используется базовым методом коррекции ошибок.

Поле *Индикатор длины (Length Indicator, LI)* (длина 6 бит) характеризует тип сигнальной единицы: LI > 2 соответствует MSU, LI = 1 или 2 соответствует LSSU, LI = 0 соответствует FISU.

Поле *Байт служебной информации (Service Information Octet, SIO)* (длина 8 бит) состоит из индикатора службы (Service Indicator, SI), используемого в MSU для привязки сигнальной информации к конкретной подсистеме пользователя, и поля подслужбы (Sub-service Field), содержащего *индикатор сети (Network Indicator, NI)*.

Поле сигнальной информации (Signaling Information Field, SIF) имеет переменную длину и содержит информацию, предоставленную верхними уровнями для передачи. Длина этого поля состоит из целого числа байт, не менее 2 и не более 272.

Поле состояния (Status Field, SF) (длина 1 или 2 байта) передаётся только в составе LSSU и содержит информацию о состоянии звена.

Поле контрольной суммы (Check Sum, CS) (длина 16 бит) используется для контроля целостности.

MTP2 выполняет следующие функции:

- инициализацию звена сигнализации;
- определение границ сигнальных единиц и их первичное кодирование/ декодирование;
- управление потоком;
- индикацию перегрузок для MTP3;
- обработку отказа управляющего процессора;
- обнаружение ошибок;
- коррекцию ошибок;
- мониторинг ошибок.

MTP3 содержит функции и процедуры управления передачей информации между различными пунктами в сети сигнализации, которые являются общими для всех звеньев сигнализации, но не зависят от их функционирования по отдельности. При помощи MTP3 осуществляются обработка сигнальных сообщений и управление сетью сигнализации.

Функции обработки сигнальных сообщений гарантируют доставку сигнальных единиц от подсистемы пользователя MTP, находящейся в *исходящем пункте сигнализации (Originating Point, OP)*, к такой же подсистеме, находящейся в *пункте назначения (Destination Point, DP)*. Эти функции базируются на поле NI в байте служебной информации (SIO) и метке маршрутизации, которые содержатся в значащих сигнальных единицах и явно определяют используемое звено сигнализации, исходящий пункт и пункт назначения.

Функции сетевого управления позволяют настраивать и гибко реконфигурировать сигнальную сеть в случае сбоев в звеньях или пунктах сигнализации, а также осуществлять контроль за сигнальным трафиком для предотвращения перегрузок.

7.3.1.2. Подсистема SCCP

Подсистема SCCP для реализации функций адресации сообщений помимо *кода пункта назначения DPC (Destination Point Code)* использует *номер подсистемы (Subsystem Number, SSN)*, который идентифицирует подсистему

пользователя SCCP внутри узла сети. Кроме того, SCCP позволяет адресовать сообщения с помощью *глобальных наименований (Global Titles, GT)*, в качестве которых могут выступать, например, цифры телефонного номера абонента.

В SCCP определены следующие услуги расширенной передачи сообщений:

- простая передача без установления соединения — информация пользователя группируется в *блоки данных (Network Service Data Unit, NSDU)*, которые доставляются функциями SCCP в пункт назначения независимо друг от друга и без учёта последовательности;
- последовательная передача без установления соединения — информация пользователя группируется в NSDU, которые доставляются функциями SCCP в пункт назначения независимо друг от друга, но с учётом последовательности;
- простая передача с установлением соединения — двунаправленная передача NSDU через установленное сигнальное соединение с возможностью обеспечения сохранения последовательности, сегментации и сборки сообщений для передачи блоков NSDU длиной более 255 байт;
- установление соединения с контролем потока данных — двунаправленная передача NSDU через установленное сигнальное соединение с возможностью управления потоком, а также обнаружением потери и нарушения последовательности сообщений.

В SCCP входят следующие функциональные блоки:

- *блок функций передачи, ориентированной на соединение (SCCP Connection-Oriented Control, SCOC)*, — контролирует установление, функционирование и разъединение сигнальных соединений;
- *блок функций передачи, не ориентированной на соединение (SCCP Connectionless Control, SCLC)*, — осуществляет передачу NSDU без установления соединения;
- *блок управления (SCCP Management, SCMG)* — осуществляет контроль за сбоями и перегрузками, возникающими в подсистемах пользователей SCCP или сигнальных маршрутах, позволяет перенаправлять сигнальные сообщения резервным подсистемам пользователя в случае недоступности основной подсистемы;
- *блок маршрутизации (SCCP Routing Control, SCRC)* — осуществляет маршрутизацию сообщений.

7.3.1.3. Подсистемы UP

Подсистемы UP генерируют и обрабатывают сигнальные сообщения, а также реализуют функции, специфические для конкретных типов UP сигнальной сети.

В зависимости от сети связи, для которой применяется система SS7, выделены следующие подсистемы UP:

- подсистема пользователя телефонии (Telephone User Part, TUP);

- подсистема пользователя сети ISDN (ISDN User Part, ISUP);
- прикладная подсистема обеспечения транзакций (Transaction Capabilities Application Part, TCAP);
- подсистема пользователя подвижной связи (Mobile Application Part, MAP);
- подсистема пользователя интеллектуальной сети (Intelligent Network Application Protocol, INAP).

Подсистема TUP. Подсистема TUP посредством обмена сообщениями обеспечивает поддержку функций управления телефонными вызовами в национальных и международных сетях. Сообщение содержит метку, код заголовка, а также один или несколько сигналов и/или индикаторов.

Метка состоит из следующих полей:

- *код точки назначения (Destination Point Code, DPC)* — указывает точку в системе сигнализации, для которой предназначено данное сообщение;
- *код точки отправления (Originating Point Code, OPC)* — указывает точку в системе сигнализации, отправившую данное сообщение;
- *код идентификации канала (Circuit Identification Code, CIC)* — указывает голосовой канал, непосредственно соединяющий точки назначения и отправления.

Код заголовка состоит из двух частей — H0 и H1. H0 идентифицирует указанную группу сообщений, а H1 содержит код сигнализации или (для более сложных сообщений) идентифицирует формат этих сообщений.

Подсистема ISUP. Подсистема ISUP определяет функции и процедуры передачи и обработки межстанционных сигналов для обеспечения служб коммутации каналов и возможностей пользователя сети ISDN.

Взаимодействие с пользователем ISDN осуществляется по протоколу управления вызовом (Call Control) Q.931 [15]. Для установления, управления и разъединения ISDN-соединений используются сообщения ISUP (рис. 7.6), передаваемые между коммутационными станциями и транзитными пунктами сигнализации.

Метка маршрутизации
Код идентификации канала
Код типа сообщения
Обязательная фиксированная часть
Обязательная переменная часть
Опциональная часть

Рис. 7.6. Формат сообщений ISUP

Поле *Метка маршрутизации (Routing Label)* является частью заголовка MTP, одинаковой для всех сообщений данного соединения.

Поле *Код идентификации канала (Circuit Identification Code, CIC)* идентифицирует канал, по которому передаётся сообщение.

Поле *Код типа сообщения (Message Type Code)* идентифицирует сообщение ISUP.

Поле *Обязательная фиксированная часть (Mandatory Fixed Part)* содержит обязательные, имеющие постоянную длину параметры для определённого типа сообщения.

Поле *Обязательная переменная часть (Mandatory Variable Part)* содержит обязательные параметры с переменной длиной.

Поле *Опциональная часть (Optional Part)* содержит необязательные параметры.

Сообщения ISUP делятся на пять категорий:

- сообщения установления соединения в прямом направлении (Forward Setup):
  - *первоначальный адрес сообщения (Initial Address Message, IAM)* — передаётся в прямом направлении для инициации занятия исходящего канала, передачи адреса и относящейся к нему информации;
  - *последующий адрес сообщения (Subsequent Address Message, SAM)* — может передаваться после сообщения IAM для передачи дополнительной информации от вызывающей стороны;
- общие сообщения установления соединения (General Setup):
  - *информационный запрос (Information Request)* — запрос дополнительной информации, относящейся к вызову;
  - *информация (Information)* — передача дополнительной информации, относящейся к вызову;
  - *сообщение продолжения (Continuity)* — передаётся в прямом направлении для индикации продолжения подключения информационного канала к следующей станции;
- сообщения установления соединения, передаваемые в обратном направлении (Backward Setup):
  - *адрес полученного сообщения (Address Complete Message, ACM)* — передаётся в обратном направлении и инициирует получение станцией назначения всей необходимой адресной информации для направления вызова вызываемой стороне;
  - *соединение (Connect)* — посылается в обратном направлении для индикации того, что вся адресная информация, необходимая для направления вызова вызываемой стороне, получена и на вызов дан ответ;
  - *прогрессивный вызов (Call Progress)* — сообщает, что событие, произошедшее в течение установления соединения, должно было относиться к вызывающей стороне;
- сообщения управления вызовом (Call Supervision):
  - *ответ (Answer)* — посылается в обратном направлении для индикации того, что на вызов получен ответ;

  - *переадресация вызова (Forward Transfer)* — сигнализирует о необходимости переадресации исходящего вызова;
  - *отключение (Release)* — сообщает, что канал, определённый сообщением, освобождён;
- сообщения управления каналом (Circuit Supervision):
  - *подтверждение отключения (Release Complete)* — передаётся в ответ на сообщение Release после освобождения канала;
  - *проверка целостности (Continuity Check Request)* — передаётся станцией, для канала которой осуществляется проверка целостности, к станции на другом конце канала, с запросом подсоединения оборудования проверки целостности;
  - *освобождение канала (Reset Circuit)* — передаётся для освобождения канала, когда из-за неисправности отсутствует сообщение Release или Release Complete;
  - *блокировка (Blocking)* — передаётся для целей техобслуживания к станции на другом конце канала, в результате чего происходит блокировка инициализации последовательных исходящих вызовов по этому каналу;
  - *разблокировка (Unblocking)* — передаётся к станции на другом конце канала для отмены состояния блокировки канала, обусловленного предварительно посланным сообщением Blocking или Group Blocking;
  - *подтверждение блокировки (Blocking Acknowledgment)* — подтверждает получение сообщения Blocking;
  - *подтверждение разблокировки (Unblocking Acknowledgment)* — подтверждает получение сообщения Unblocking;
  - *сообщение приостановления (Suspend)* — используется для индикации временного отключения абонентского терминала;
  - *сообщение возобновления соединения (Resume)* — сообщение о восстановлении соединения после Suspend;
- сообщения управления группой каналов (Circuit Group Supervision):
  - *блокирование группы каналов (Circuit Group Blocking)* — передаётся для целей техобслуживания к станции на другом конце группы каналов, в результате чего происходит блокировка последовательных исходящих вызовов по каналам этой группы;
  - *разблокирование группы каналов (Circuit Group Unblocking)* — передаётся к станции на другом конце группы каналов для отмены состояния блокировки группы каналов, обусловленного предварительно посланным сообщением Circuit Group Blocking;
  - *подтверждение блокировки группы каналов (Circuit Group Blocking Acknowledgment)* — подтверждает получение сообщения Circuit Group Blocking;
  - *подтверждение разблокировки группы каналов (Circuit Group Unblocking Acknowledgment)* — подтверждает получение сообщения Circuit Group Unblocking;
  - *перезапуск группы каналов (Circuit Group Reset)* — передаётся для освобождения группы каналов, когда из-за неисправности невозможно опре-

делить, каким каналам соответствуют сигналы освобождения;
– *подтверждение перезапуска группы каналов (Circuit Group Reset Acknowledgment)* — передаётся в ответ на сообщение перезапуска группы каналов.

Подсистема TCAP. Подсистема TCAP предназначена для взаимодействия сетевых приложений. В сетях связи распределённые приложения, использующие TCAP, обычно функционируют на коммутационных станциях и в сетевых базах данных. Основной функцией TCAP в этих сетях является вызов удалённых процедур для поддержки услуг интеллектуальной сети.

TCAP разделена на два подуровня: *подуровень компонент (Component Sublayer, CSL)* и *подуровень транзакций (Transaction Sublayer, TSL)*. Подуровень компонент осуществляет обмен компонент (запрос на действие на удалённом конце или ответ на вызванную операцию) между транзакциями пользователей. Подуровень транзакций ответственен за обмен сообщениями, которые содержат эти компоненты.

Для TCAP определены следующие типы сообщений:
– безадресное сообщение (Undirectional);
– сообщение начала (Begin);
– сообщение продолжения (Continue);
– сообщение окончания (End);
– сообщение прерывания (Abort).

Для TCAP определены следующие типы компонент:
– вызов (Invoke);
– возвращение результата (Return Result);
– возвращение ошибки (Return Error);
– отказ (Reject).

Подсистема MAP. Подсистема MAP обеспечивает выполнение процедур сигнализации, необходимых для обмена информацией в сетях сотовой подвижной связи, например стандарта GSM.

Сообщения MAP передаются между мобильными коммутаторами и базами данных для поддержки аутентификации пользователей, идентификации оборудования и роуминга. Передача сообщений осуществляется с помощью протокола TCAP.

7.3.2. Преимущества и недостатки SS7

Система SS7 обладает следующими преимуществами:
– оптимизирована для работы в цифровых сетях связи в сочетании со станциями с программным управлением (Stored Program Control), но может работать и в аналоговых сетях на скорости до 64Кбит/с;
– обеспечивает надёжные средства передачи информации в правильной последовательности, без потерь или дублирования;

- имеет чёткую функциональную архитектуру, которая обеспечивает гибкость и модульность для различных применений при сохранении единой концепции системы;
- может использовать наземные и спутниковые физические каналы передачи данных.

Глава 8. Поколения беспроводных сетей

Буква «G» в названии беспроводной сети передачи данных означает «поколение».

8.1. Поколение 1G

Появившиеся в начале 1980-х годов новаторские для того времени технологии AMPS в США и сочетание TACS и NMT в Европе позволили мобильным телефонам стать массовым продуктом. Поэтому тройку AMPS, TACS и NMT принято считать первым поколением (1G).

Поколение 1G представляет исключительно аналоговые системы, разработанные в основном для осуществления голосовых вызовов. Во всех аналоговых стандартах применяются амплитудная модуляция для передачи речи и частотная модуляция для передачи управляющей информации (сигнализации).

Передача данных была возможна посредством модемных соединений. Беспроводная связь более подвержена шумам и искажениям, чем обычная проводная, поэтому скорость передачи данных была крайне низкой. Для передачи информации различных каналов используются различные участки спектра частот — применяется метод множественного доступа с частотным разделением каналов (Frequency Division Multiple Access, FDMA), с полосами каналов в различных стандартах от 12,5 до 30 кГц. С этим непосредственно связан основной недостаток аналоговых систем — относительно низкая ёмкость, являющаяся прямым следствием недостаточно рационального использования выделенной полосы частот при частотном разделении каналов. Кроме того, стоимость минуты разговора в 80-х гг. XX в. была такой высокой, что мобильный телефон мог считаться роскошью.

8.2. Поколение 2G

Начало 1990-х годов ознаменовалась началом развития цифровых сотовых сетей связи, имеющих ряд преимуществ по сравнению с аналоговыми системами. Основные преимущества — улучшенное качество звука, большая защищенность, повышенная мощность передатчика. В Европе развивалась технология GSM, в США — D-AMPS и ранняя версия CDMA компании Qualcomm. Цифровые системы второго поколения основаны на методе множественного доступа с временным разделением каналов (Time Division Multiple Access, TDMA).

Сети поколения 2G поддерживают такие услуги как передача коротких текстовых сообщений (Short Messaging Service, SMS), передачи данных с коммутацией каналов (Circuit Switched Data, CSD).

Для того, чтобы инициировать передачу данных с помощью технологии CSD, необходимо было совершить специальный «вызов», что было похоже на соединение по телефонному модему — вы или были подключены к сети, или нет. В условиях того, что тарифные планы в то время измерялись в десятках минут, а CSD была сродни обыкновенному звонку, практической пользы от технологии почти не было.

8.3. Поколение 2.5G

Появление услуги «General Packet Radio Service» (GPRS) в 1997 году стало переломным моментом в истории сотовой связи. GPRS представляет собой технологию непрерывной передачи данных для GSM сетей. GPRS может работать с большей, чем CSD, скоростью — теоретически до 100 кБит/с. При этом операторы получили возможность тарифицировать трафик, а не время на линии.

GPRS появился в очень подходящий момент — в период широкого использования электронной почты (e-mail). Но это нововведение не позволило добавить единицу к поколению мобильной связи. В то время, как технология GPRS уже была на рынке, Международный Союз Электросвязи (ITU) предложил новый стандарт — IMT-2000 — утверждающий спецификации «настоящего» 3G. Ключевым моментом стало обеспечение скорости передачи данных 2 МБит/с для стационарных терминалов и 384 кБит/с для мобильных.

Таким образом, GPRS застрял между поколениями 2G, которое он превосходил, и 3G, до которого не дотягивал. Это стало началом раскола поколений.

8.4. Поколение 3G

Помимо более высокой скорости передачи спецификации 3G обеспечили достаточно лёгкую миграцию с сетей второго поколения.

На смену GSM пришла универсальная мобильная телекоммуникационная система (Universal Mobile Telecommunications System, UMTS). Способ передачи данных — широкополосный множественный доступ с кодовым разделением (Wideband Code Division Multiple Access, W-CDMA). Скорость передачи информации — до 2 Мбит/с.

В 1992–1993 гг. в США был разработан стандарт системы сотовой связи на основе метода множественного доступа с кодовым разделением каналов (Code Division Multiple Access, CDMA). На смену ему пришёл стандарт CDMA2000, продвигаемый американским оператором Qualcomm. CDMA2000 имеет 2 фазы развития: первая 1XRTT (One Times Radio Transmission Technology), также известная как 1X, обеспечивает скорость передачи данных до 144 Кбит/с, и может быть усовершенствована до второй фазы — 3XRTT (или 3X), где скорость достигает 2 Мбит/с.

Стандарт цифровой технологии беспроводной передачи данных Enhanced Data-rates for GSM Evolution (EDGE) — был задуман как легкий способ опера-

торов сетей GSM получить дополнительные возможности от 2.5G установок, не вкладывая серьезные деньги в обновление оборудования. С помощью телефона, поддерживающего EDGE, можно получить скорость, в два раза превышающую GPRS, что вполне неплохо для того времени. Многие европейские операторы не стали возиться с EDGE и были приверженцами внедрения UMTS.

Итак, куда же отнести EDGE? Это не так быстро, как UMTS или EV-DO, так что вы можете сказать, что это не 3G. Но это явно быстрее, чем GPRS, что означает, что она должна быть лучше, чем 2.5G, не так ли? Действительно, многие люди назвали бы EDGE технологией 2.75G.

Спустя десятилетие, сети CDMA2000 получили обновление до EV-DO Revision A, которая предлагает немного более высокую входящую скорость и намного выше исходящую скорость. В оригинальной спецификации, которая называется EV-DO Revision 0, исходящая скорость ограничена на уровне 150 кБит/с, новая версия позволяет делать это в десять раз быстрее. Таким образом, мы получили 3.5G! То же самое для UMTS: технологии HSDPA (High-Speed Downlink Packet Access) и HSUPA (High-Speed Uplink Packet Access) позволили добавить скорость для входящего и исходящего трафика.

Дальнейшие усовершенствования UMTS используют HSPA+, dual-carrier HSPA+, и HSPA+ Evolution, которые теоретически обеспечивают пропускную способность от 14 МБит/с до 600 МБит/с. Итак, можно ли сказать что мы попали в новое поколение, или это можно назвать 3.75G по аналогии с EDGE и 2.75G?

8.5. Поколение 4G

Подобно тому, как было со стандартом 3G, ITU взяла под свой контроль 4G, привязав его к спецификации, известной как IMT-Advanced. Документ призывает к скорости входящих данных в 1 ГБит/с для стационарных терминалов и 100 МБит/с для мобильных. Это в 500 и 250 раз быстрее по сравнению с IMT-2000. Это действительно огромные скорости, которые могут обогнать рядовой DSL-модем или даже прямое подключение к широкополосному каналу.

Беспроводные технологии играют ключевую роль в обеспечении широкополосного доступа в сельской местности. Это более рентабельно — построить одну станцию 4G, которая обеспечит связь на расстоянии десятков километров, чем покрывать сельхозугодья одеялом из оптоволоконных линий.

К сожалению, эти спецификации являются настолько агрессивными, что ни один коммерческий стандарт в мире не соответствует им. Исторически сложилось, что технологии WiMAX и Long-Term Evolution (LTE), которые призваны добиться такого же успеха как CDMA2000 и GSM, считаются технологиями четвертого поколения, но это верно лишь отчасти: они оба используют новые, чрезвычайно эффективные схемы мультиплексирования (OFDMA, в отличие от старых CDMA или TDMA которые мы использовали на протяжении последних двадцати лет) и в них обоих отсутствует канал

для передачи голоса. 100 процентов их пропускной способности используется для услуг передачи данных. Это означает, что передача голоса будет рассматриваться как VoIP. Учитывая то, как сильно современное мобильное общество ориентировано на передачу данных, можно считать это хорошим решением.

Где WiMAX и LTE терпят неудачу, так это в скорости передачи данных, у них эти значения теоретически находятся на уровне 40 МБит/с и 100 МБит/с, а на практике реальные скорости коммерческих сетей не превышают 4 МБит/с и 30 МБит/с соответственно, что само по себе очень неплохо, однако не удовлетворяет высоким целям IMT-Advanced. Фактически требованиям 4G соответствуют лишь обновления этих стандартов — WiMAX 2 и LTE-Advanced.

Тем не менее, можно утверждать, что оригинальные стандарты WiMAX и LTE достаточно отличаются от классических стандартов 3G, чтобы можно было говорить о смене поколений. И действительно, большинство операторов по всему миру, которые развернули подобные сети, называют их 4G. Очевидно, это используется в качестве маркетинга, и организация ITU не имеет полномочий противодействовать.

Итак, что же это все нам дает? Похоже, операторы выиграли эту битву: ITU недавно отступил, заявив, что термин 4G «может быть применен к предшественникам этой технологии, LTE и WiMAX, а также другим эволюционировавшим 3G технологиям, обеспечивающим существенное повышение производительности и возможностей по сравнению с начальной системой третьего поколения». Так называемые «4G» сети сегодня напоминают сети 3G 2001 года. Можно передавать потоковое видео очень высокого качества, загружать большие файлы в мгновение ока и даже, в определенных условиях, использовать некоторые из этих сетей как замену DSL.

Глава 9. Сети 2G

9.1. GSM

Global System for Mobile Communications (GSM) — стандарт цифровой мобильной сотовой связи с разделением каналов по времени (Time Division Multiple Access, TDMA) и частоте (Frequency Division Multiple Access, FDMA). GSM относится к сетям поколения 2G (цифровая сотовая связь).

Система GSM совместима с ISDN по услугам и используемым сигналам управления. GSM поддерживает синхронные и асинхронные потоки данных как однонаправленный сервис через терминалы ISDN. GSM может работать со скоростями связи 300, 600, 1200, 2400 и 9600 бит/с.

Услуги GSM:

- телефонная связь (передача речи);
- передача коротких сообщений (Short Message Service, SMS);
- передача данных (General Packet Radio Service, GPRS);
- голосовая почта;
- международный роуминг (roaming);
- идентификация звонящего;
- перенаправление вызова (call forwarding);
- ожидание вызова (call waiting);
- конференц-связь (multiparty conversations);
- возможность отключения исходящих (международных) вызовов и др.

9.1.1. Структура GSM

Основные уровни системы:

- подсистема базовых станций (Base Station Subsystem, BSS);
- подсистема коммутации (Network Switching Subsystem, NSS);
- центр технического обслуживания (Operation and Maintenance Centre, OMC).

9.1.1.1. Элементы подсистемы базовых станций

Базовая станция (Base Transceiver Station, BTS) обеспечивает приём/передачу сигнала между мобильной станцией (Mobile Station, MS) и контроллером базовых станций (Base Station Controller, BSC).

Контроллер базовой станции (BSC) контролирует соединения между базовой станцией (BTS) и подсистемой коммутации (NSS).

Функции контроллера базовой станции (BSC):

- управление очерёдностью соединений;
- управление скоростью передачи данных;
- распределение радиоканалов;

– сбор статистики;
– контроль различных радиоизмерений;
– назначение и управление процедурой Handover.

9.1.1.2. Элементы подсистемы коммутации

Центр коммутации (Mobile Switching Centre, MSC):
– контролирует определённую географическую зону с расположенными на ней базовыми станциями (BTS) и контроллерами базовых станций (BSC);
– устанавливает соединение к абоненту и от него внутри сети GSM;
– обеспечивает интерфейс между GSM и ТфОП, другими сетями радиосвязи, сетями передачи данных;
– обеспечивает выполнение функции маршрутизации вызовов, управления вызовами, эстафетной передачи обслуживания при перемещении мобильной станции (MS) из одной ячейки в другую;
– обрабатывает данные по вызову и передаёт их в центр расчётов для формирования счета за предоставленные услуги, собирает статистические данные;
– следит за положением мобильной станции (MS).

Типы MSC:
– шлюзовой MSC (Gate MSC, GMSC) — обрабатывает вызовы, приходящие из внешних сетей;
– абонентский MSC (Visited MSC) — MSC, в зоне действия которого находится абонент;
– исходный MSC (Anchor MSC) — инициирует процедуру хендовера;
– целевой MSC — это MSC на который должен пройти хендовер.

Домашний регистр местоположения (Home Location Registry, HLR) содержит базу данных приписанных к нему абонентов:
– информация о предоставляемых определённому абоненту услугах;
– информация о состоянии каждого абонента (доступность, платёжеспособность и пр.);
– *международный идентификатор мобильного абонента (International Mobile Subscriber Identity, IMSI)*;
– *номер мобильного абонента цифровой сети с интеграцией служб (Mobile Station Integrated Services Digital Number, MSISDN)*.

Гостевой регистр местоположения (Visitor Location Registry, VLR) обеспечивает мониторинг передвижения мобильной станции (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». При перемещении абонента в другую зону данные о нём удаляются из гостевого регистра местоположения (VLR).

Регистр идентификации оборудования (Equipment Identification Registry, EIR) содержит базу данных, необходимую для установления подлинности мобильной станции (MS) по *международному идентификатору мобильного оборудования (International Mobile Equipment Identity, IMEI)*.

Центр аутентификации (Authentification Centre, AUC) осуществляет процедуру проверки подлинности абонента по данным *SIM-карты (Subscriber Identity Module)*.

9.1.1.3. Подсистема центра технического обслуживания

- обеспечивает контроль качества работы и управление всей сетью;
- обрабатывает аварийные сигналы;
- обеспечивает проверку состояния сети, возможность прохождения вызова;
- производит обновление программного обеспечения на всех элементах сети и ряд других функций.

9.1.1.4. Другие элементы сети GSM

SMS-центр (SMS Centre, SMSC) отвечает за работу службы коротких сообщений сети мобильной связи.

Узел обслуживания абонентов GPRS (Serving GPRS Support Node, SGSN) — реализует все функции обработки пакетной информации.

Системный центр мультимедийных сообщений (Multimedia Messaging System Centre, MMSC) обеспечивает отправку мультимедийных сообщений — MMS (например, изображения, аудио, видео или их комбинации).

9.1.2. Протоколы GSM

9.1.2.1. BSS Application Part

Между центрами коммутации MSC (Mobile Services Switching Center) и базовыми станциями BSS (Base Station System) для поддержки сигнальных сообщений используются протоколы MTP и SCCP.

Определена одна пользовательская функция SCCP, называемая *BSS Application Part (BSSAP)*. В случае соединений «точка-точка» BSSAP использует одно сигнальное соединение на активную мобильную станцию, имеющую одну или несколько транзакций передачи сообщений уровня 3 (сетевой). В этом случае для голосовой группы или широковещательного вызова всегда организуется одно соединение на соту, участвующую в данном вызове, и одно дополнительное соединение на BSS для передачи сообщений уровня 3. Существует также дополнительное соединение (для говорящего при широковещательном соединении или для первого заговорившего в голосовой группе) с точкой, которую сеть планирует использовать для передачи в общий канал. Дополнительное соединение может также потребоваться для любой мобильной станции в голосовой группе или широковещательном соединении, которую сеть решит поместить на отдельное соединение.

BSSAP поддерживает две пользовательские функции:

- *Direct Transfer Application sub-Part (DTAP или GSM L3)* используется для передачи сообщений между MSC и MS (мобильная станция); информация

сетевого уровня в этих сообщениях не интерпретируется BSS. Описания протоколов сетевого уровня для информационного обмена MS-MSC содержатся в серии 04-технических спецификаций GSM;
- *BSS Management Application sub-Part (BSSMAP)* поддерживает другие процедуры между MSC и BSS, связанные MS (управление ресурсами, контроль передачи) сотами с BSS или BSS в целом. Описание протокола сетевого уровня для информационного обмена BSSMAP содержится в рекомендациях GSM 08.08.

Для поддержки BSSMAP используются как процедуры на базе соединений, так и процедуры, не требующие организации соединения. Ориентированные на соединения процедуры используются для поддержки DTAP. Функция распределения, локализованная в BSSAP, которая отражена в спецификации протокола заголовком уровня 3, обеспечивает разделение данных, связанных с двумя субпротоколами (subpart).

9.1.2.2. Direct Transfer Application sub-Part (DTAP)

DTAP (Direct Transfer Application Part) используется для передачи сообщений управления звонками и управляющих сообщений между MSC и MS.

Формат заголовка DTAP:

- дискриминатор протокола (4 бита): указывает на протокол сетевого уровня, к которому относятся сообщения уровня 3:
  - 0000 — управление групповыми вызовами;
  - 0001 — управление широковещательными вызовами;
  - 0010 — PDSS1;
  - 0011 — управление вызовами и связанные с вызовами сообщения SS;
  - 0100 — PDSS2;
  - 0101 — управляющие сообщения Mobility Management;
  - 0110 — сообщения управления радио-ресурсами;
  - 1001 — сообщения SMS;
  - 1011 — не связанные с вызовами сообщения SS;
  - 1110 — расширение PD на один октет;
  - 1111 — тестовые процедуры, описанные в TS GSM 11.10.
- идентификатор транзакции / пропуска (4 бита): содержит значение транзакции и флаг, который показывает кому он выделен;
- N(SD):
  - для MM и CM поле N(SD) устанавливает значение переменной состояния передачи (send state);
  - для других сообщений сетевого уровня бит 7 устанавливается в 0 передающей стороной;
  - сообщения, у которых бит 7 имеет значение 1, игнорируются.
- идентификатор типа сообщения сетевого уровня GSM (1 байт);
- информационные элементы.

9.1.2.3. BSS Management Application Part

BSSMAP (BSS Management Application Part) поддерживает все процедуры между MSC и BSS, которые требуют интерпретации и обработки информации, связанной с отдельными звонками и управлением ресурсами. Некоторые процедуры BSSMAP переключаются управляющими сообщениями RR (Radio Resource), определенными в GSM 04.08 или инициируют такие сообщения.

Формат заголовка BSSMAP:

- тип сообщения (1 байт): задаёт тип (функции и формат) каждого сообщения BSSMAP;
- информационные элементы (2-n байт): имеет идентификатор размером в 1 октет (байт).

9.1.2.4. Протокол Base Transceiver Station Message (BTSM)

BTSM — протокол взаимодействия между контроллером базовой станции (Base Station Controller) и трансивером базовой станции (Base Transceiver Station).

Формат заготовка BTSM:

- дискриминатор сообщений (1 байт): различает сообщения Transparent и Non-Transparent, Radio Link Layer Management (управление радиоканалом, 0000001), Dedicated Channel Management (управление выделенным каналом, 0000100), Common Channel Management (управление общим каналом, 0000110) и TRX Management (управление TRX, 0001000);
- тип сообщения (1 байт):
  - 0001 xxxx — сообщения управления радиоканалом:
    - 0001 — запрос данных (DATA REQuest);
    - 0010 — индикация данных (DATA INDication);
    - 0011 — ошибка индикации (ERROR INDication);
    - 0100 — запрос на установление соединения (ESTablish REQuest);
    - 0101 — установление соединения закончено (ESTablish CONfirm);
    - 0110 — индикация установления соединения (ESTablish INDication);
    - 0111 — запрос на освобождение радиоканала (RF CHANnel RELease REQuest);
    - 1000 — освобождение радиоканала закончено (RF CHANnel RELease CONfirm);
    - 1001 — индикация освобождения (RELease INDication);
    - 1010 — запрос блока данных (UNIT DATA REQuest);
    - 1011 — индикация блока данных (UNIT DATA INDication);
  - 0110 xxxx — сообщения управления общим каналом / TRX:
    - 0001 — информация BSSCH (BCCH INFOrmation);
    - 0010 — загрузка индикации CCCH (CCCH LOAD INDication)
    - 0011 — запрошен канал (CHANnel ReQuireD);
    - 0100 — удаление индикации (DELETE INDication);
    - 0101 — широковещательная команда (PAGING CoMannD);

  - 0110 — команда срочного назначения (IMMEDIATE ASSIGN COMMAND);
  - 0111 — команда широковещательного SMS (SMS BroadCast REQuest);
  - 1001 — индикация ресурса радио частот (RF RESource INDication);
  - 1010 — заполнение SACCH (SACCH FILLing);
  - 1011 — перезагрузка (OVERLOAD);
  - 1100 — отчёт об ошибках (ERROR REPORT);
  - 1101 — команда широковещательного SMS (SMS BroadCast CoMannD);
  - 1110 — загрузка индикации BSCCH (BCCH LOAD INDication);
  - 1111 — команда извещения (NOTification CoMannD);
- 100 xxxxx — сообщения управления выделенным каналом:
  - 00001 — активизация канала (CHANnel ACTIVation);
  - 00010 — подтверждение активизации канала (CHANnel ACTIVation ACKnowledge);
  - 00011 — отрицательное подтверждение активизации канала (CHANnel ACTIVation Negative ACK);
  - 00100 — ошибка подключения (CONNECTION FAILure);
  - 00101 — деактивизация SACCH (DEACTIVATE SACCH);
  - 00110 — команда шифрования (ENCRyption CoMmanD);
  - 00111 — определение хэндовера (HANDOver DETection);
  - 01000 — результат измерений (MEASurement RESult);
  - 01001 — запрос режима модификации (MODE MODIFY REQuest);
  - 01010 — подтверждение режима модификации (MODE MODIFY ACKnowledge);
  - 01011 — MODE MODIFY Negative ACK;
  - 01100 — PHYsical CONTEXT REQuest;
  - 01101 — PHYsical CONTEXT CONFirm;
  - 01110 — RF CHANnel RELease;
  - 01111 — MS POWER Control;
  - 10000 — BS POWER Control;
  - 10001 — PREPROCess CONFIGure;
  - 10010 — PREPROCessed MEASurement RESult;
  - 10011 — RF CHANnel RELease ACKnowledge;
  - 10100 — SACCH INFO MODIFY;
  - 10101 — TALKER DETection;
  - 10110 — LISTENER DETection;
- информационные элементы.

9.1.2.5. Протокол Radio Resource (RR)

Процедуры RR:

- выбор сот;
- передача данных.

Основная задача процедур RR — организация, поддержка (управление) и разрыв соединений RR, которые в свою очередь организуют диалог между сетью и мобильной станцией в режиме «точка-точка».

Функции RR:

- управление физическими каналами связи;
- управление соединением канального уровня на каналах управления и др.

Формат заголовка RR:

- дискриминатор протокола (4 бита): имеет значение 0110 и идентифицирует протокол управления RR;
- идентификатор пропуска (4 бита): имеет значение 0000;
- тип сообщения (8 бит): определяет назначение и формат каждого сообщения RR:
  - 00111 xxx — сообщения организации каналов:
    - 011 — дополнительное распределение (ADDitional ASSignment);
    - 111 — непосредственное распределение (IMMdiate ASSignment);
    - 001 — непосредственное расширенное распределение (IMMdiate ASSignment EXTended);
    - 010 — непосредственное распределение отклонено (IMMdiate ASSignment REJect)
  - 00110 xxx — сообщения о шифровании:
    - 101 — команда режима шифрования (Ciphering MODE CoMmanD);
    - 010 — режим шифрования закончен (Ciphering MODE COMplete);
  - 00101 xxx — сообщения, связанные с передачей:
    - 110 — команда распределения (ASSignment CoMmanD);
    - 001 — распределение закончено (ASSignment COMplete);
    - 111 — ошибка распределения (ASSignment FAILure);
    - 011 — команда хэндовера (HANDover CoMmanD);
    - 100 — хэндовер закончен (HANDover COMplete);
    - 000 — ошибка хэндовера (HANDover FAILure);
    - 101 — физическая информация (PHYSical INFormation);
  - 00001 xxx — сообщения закрытия каналов:
    - 101 — освобождение канала (CHANnel RELease);
    - 010 — частичное освобождение (PARTial RELease);
    - 111 — частичное освобождение закончено (PARTial RELease COMplete);
  - 00100 xxx — широковещательные-сообщения:
    - 001 — PAGING REQUEST TYPE 1;
    - 010 — PAGING REQUEST TYPE 2;
    - 100 — PAGING REQUEST TYPE 3;
    - 111 — PAGING RESPONSE (ответ на сообщения);
  - 00011 xxx — системные сообщения:
    - 000 — SYSTEM INFORMATION TYPE 8;
    - 001 — SYSTEM INFORMATION TYPE 1;
    - 010 — SYSTEM INFORMATION TYPE 2;
    - 011 — SYSTEM INFORMATION TYPE 3;
    - 100 — SYSTEM INFORMATION TYPE 4;

  - 101 — SYSTEM INFORMATION TYPE 5;
  - 110 — SYSTEM INFORMATION TYPE 6;
  - 111 — SYSTEM INFORMATION TYPE 7;
- 00000 xxx — системные информационные сообщения:
  - 010 — SYSTEM INFORMATION TYPE 2bis;
  - 011 — SYSTEM IN FORMATION TYPE 2ter;
  - 101 — SYSTEM INFORMATION TYPE 5bis;
  - 110 — SYSTEM INFORMATION TYPE 5ter;
- 00010 xxx — различные сообщения:
  - 000 — модификация режима канала (CHANnel MODE MODify);
  - 010 — статус RR (RR STATUS);
  - 111 — подтверждение модификации режима канала (CHANnel MODE MODify ACKnowledge);
  - 100 — перераспределение частот (FREQuency REDEFinition);
  - 101 — отчёт об измерении (MEASurement REPort);
  - 110 — изменение набора услуг (CLASSMARK CHANGE);
  - 011 — запрос набора услуг (CLASSMARK ENQuiry);
- информационные элементы (3-n байт).

9.1.2.6. Протокол Mobility Management (MM)

Основная задача MM (Mobility Management) — поддержка мобильности пользовательских терминалов.

Функции MM:

- информирование сети о местоположении мобильных пользователей;
- обеспечение конфиденциальности идентификации пользователей;
- обеспечение услуг поддержки соединений с различными объектами подуровня управления соединениями (CM).

Формат заголовка MM:

- дискриминатор протокола (4 бита): имеет значение 0101 и идентифицирует протокол MM;
- идентификатор пропуска (4 бита): имеет значение 0000;
- тип сообщения:
  - 0x00 xxxx — регистрационные сообщения:
    - 0001 — выделен индикатор IMSI (IMSI DETuch INDicator);
    - 0010 — изменение местоположения принято (LOCation UPDate ACcept);
    - 0100 — изменение местоположения отклонено (LOCation UPDate REJect);
    - 1000 — запрос на изменение местоположения (LOCation UPDate REQuest);
  - 0x01 xxxx — сообщения, связанные с безопасностью:
    - 0001 — аутентификация отклонена (AUTHentication REJect);
    - 0010 — запрос на аутентификацию (AUTHentication REQuest);
    - 0100 — ответ на аутентификацию (AUTHentication RESponse);

  - 1000 — запрос на идентификацию (IDENtification REQuest);
  - 1001 — ответ на идентификацию (IDENtification RESponse);
  - 1010 — команда на изменение TSMI (TSMI REALlOCation CoMmanD);
  - 1011 — изменение TSMI закончено (TSMI REALlOCation COMplete);
- 0x10 xxxx — сообщения управления соединениями:
  - 0001 — услуги CM приняты (CM SERVice ACCept);
  - 0010 — услуги CM отклонены (CM SERVice REJ ect);
  - 0011 — услуги CM прерваны (CM SERVice ABORT);
  - 0100 — запрос услуг CM (CM SERVice REQuest);
  - 1000 — изменение услуг CM (CM SERVice REESTABlishment);
  - 1001 — прерывание (ABORT);
- 0x11 xxxx — различные сообщения:
  - 0100 — состояние MM (MM STATUS);
- информационные элементы.

9.1.2.7. Протокол Call Control

Протокол управления соединениями (Call Control, CC) является одним из протоколов подуровня CM (Connection Management). Каждая мобильная станция должна поддерживать протокол управления соединениями. Если мобильная станция не поддерживает какую-либо из возможностей, такая станция должна ответить на сообщение SETUP сообщением RELEASE COMPLETE. В протоколе управления соединениями определено множество объектов CC. Каждый объект CC независим от других объектов и связывается только с соответствующим объектом того же уровня, используя собственное соединение MM.

Структура CC:

- дискриминатор протокола (4 бита): имеет значение 0011 и указывает на протокол CC;
- идентификатор транзакции (4 бита): позволяет различить одновременные операции (транзакции) в одной мобильной станции:
  - флаг TI (1 бит): указывает, кто выделил значение TI для данной транзакции;
  - значение TI (3 бита): выделяется стороной интерфейса, инициировавшей транзакцию;
- тип сообщения (1 байт):
  - бит 8 зарезервирован для использования в будущем (бит расширения);
  - бит 7 зарезервирован для передачи порядкового номера в сообщениях от мобильных станций;
  - сообщения CC могут иметь следующие типы:
    - 0x00 0000 — переход к национальным типам сообщений;
    - 0x00 xxxx — сообщения организации соединений:
      - 0001 — оповещение (ALERting);
      - 1000 — вызов выполнен (CALL CONFIRMED);

  - 0010 — вызов обслуживается (CALL PROCeeding);
  - 0111 — соединить (CONnect);
  - 1111 — подтверждение соединения (CONnect ACKnowledge);
  - 1110 — аварийный вызов (EMERGence SETUP);
  - 0011 — PROGRESS;
  - 0101 — вызов (SETUP);
- 0x01 xxxx — сообщения информационной фазы соединений:
  - 0111 — модификация (MODify);
  - 1111 — модификация закончена (MODify COMplete);
  - 0011 — отказ в модификации (MODify REJect);
  - 0000 — информация пользователя (USER INFormation);
  - 1000 — удержание (HOLD);
  - 1001 — подтверждение удержания (HOLD ACKnowledge);
  - 1010 — отказ от удержания (HOLD REJect);
  - 1100 — возобновление (RETRieve);
  - 1101 — подтверждение возобновления (RETRieve ACKnowledge);
  - 1110 — отказ от возобновления (RETRieve REJect);
- 0x10 xxxx — сообщения разрыва соединений:
  - 0101 — разъединение (DISConnect);
  - 1101 — освобождение (RELease);
  - 1010 — освобождение закончено (RELease COMplete);
- 0x11 xxxx — прочие сообщения:
  - 1001 — управление перегрузкой (CONGestion Control);
  - 1110 — извещение (NOTIFY);
  - 1101 — статус (STATUS);
  - 0100 — запрос статуса (STATUS ENQuiry);
  - 0101 — начало частотного набора (START DTMF);
  - 0001 — остановка частотного набора (STOP DTMF);
  - 0010 — подтверждение остановки частотного набора (STOP DTMF ACKNOWLEDGE);
  - 0110 — подтверждение начала частотного набора (START DTMF ACKNOWLEDGE);
  - 0111 — отмена начала частотного набора (START DTMF REJECT);
  - 1010 — обращение к дополнительным услугам (FACILITY);

9.2. CDMA

CDMA - Code Division Multiplie Access (Множественный доступ с кодовым разделением)

Группа стандартов *CDMA (Code Division Multiplie Access, множественный доступ с кодовым разделением)* использует технологию Direct Sequence (Pseudo Noise) Spread Spectrum (прямая последовательность (псевдошум) с широким спектром). Основа DSSS — использование шумоподобной несущей, и гораздо более широкой полосы, чем необходимо для обычных способов модуляции. Хотя DSSS была изобретена ещё в 1940-е, коммерческое при-

менение началось только в 1995 году. Причиной тому — отсутствие технологий позволяющих создавать малогабаритные приёмопередатчики использующие DSSS.

Представим себе узкополосный сигнал промодулированный неким потоком данных со скоростью, например 9600 bps. Пусть есть уникальная, повторяющаяся, псевдослучайная цифровая последовательность со значительно большей скоростью, скажем 1.25 Mbps. Если менять фазу узкополосного сигнала в соответствии с псевдослучайной последовательностью, то мы получим шумоподобный сигнал с широким спектром, содержащий в себе информацию. Если рассмотреть, что происходит с точки зрения частоты — то получится что информационный сигнал расплылся (spread) по спектру шумоподобного сигнала (pseudonoise). Теперь осталось выдать этот широкополосный сигнал в эфир.

На пути от передатчика к приёмнику к сигналу добавятся помехи и сигналы других передатчиков. Принятый и демодулированный сигнал перемножим с точной копией шумоподобного сигнала, который использовался для модуляции (здесь необходима очень высокая степень синхронизации приёмника и передатчика) и получим узкополосную составляющую с высокой энергией на единицу частоты - переданный поток данных. Так как помехи и сигналы от других передатчиков не совпадают с использованным шумоподобным сигналом, то после перемножения они ещё больше расползутся по спектру и их энергия на единицу частоты уменьшится.

Таким образом, используя разные псевдослучайные последовательности (коды) можно организовать несколько независимых каналов передачи данных в одной и той же полосе частот.

В системах с частотным разделением каналов (как в FDMA, так и в TDMA) существует проблема так называемого многократного использования (reuse) частотных каналов. Чтобы не мешать друг другу, соседние базовые станции должны использовать разные каналы. Таким образом, если у БС 6 соседей (наиболее часто рассматриваемый случай, при этом зону каждой БС можно представить как шестиугольник, а всё вместе выглядит как пчелиные соты) то количество каналов, которые может использовать эта БС в семь раз меньше чем общее количество каналов в отведённом для сети диапазоне. Это приводит к уменьшению ёмкости сети и необходимости увеличивать плотность установки БС в густонаселённых районах. Для CDMA такой проблемы вообще нет. Все БС работают на одном и том же канале. Таким образом, частотный ресурс используется более полно. Ёмкость CDMA сети обычно в несколько раз выше, чем TDMA, и на порядок выше чем FDMA сетей.

Для того, чтобы телефоны находящиеся близко к БС не забивали своим сигналом более отдалённых абонентов, в CDMA предусмотрена плавная регулировка мощности, что приводит к значительному сокращению энергопотребления телефона вблизи БС и, соответственно, увеличению времени работы телефона без подзарядки.

Одной из особенностей CDMA сетей является возможность мягкого перехода от одной БС к другой (soft handoff). При этом, возможна ситуация

когда одного абонента ведут сразу несколько БС. Абонент просто не заметит, что его передали другой БС. Естественно, чтобы такое стало возможным, необходима прецизионная синхронизация БС. В коммерческих системах это достигается использованием сигналов времени от *GPS (Global Positioning System)* — американской спутниковой системы определения координат.

CDMA это практически полностью цифровой стандарт. Обычно все преобразования информационного сигнала происходят в цифровой форме, и только радиочасть аппарата является аналоговой, причём гораздо более простой, чем для других групп стандартов. Это позволяет практически весь телефон выполнить в виде одной микросхемы с большой степенью интеграции, тем самым значительно снизив стоимость телефона.

Стандарты CDMA используют более современный кодек для оцифровки речи, что субъективно повышает качество передачи аналогового сигнала по сравнению с действующими TDMA стандартами.

Из минусов CDMA можно отметить необходимость использования достаточно широкой и неразрывной полосы, что не всегда возможно в современной обстановке дефицита частотного ресурса и большую сложность реализации данной технологии.

Стандарты CDMA изначально включали в себя функцию передачи данных и на сегодня, почти все современные CDMA телефоны способны предоставлять пользователю 14.4 Kbps цифровой канал. А сама сеть использует IP протокол для передачи данных.

У CDMA гораздо меньше проблем с переходом к 3-му поколению по сравнению с TDMA системами. TIA/EIA (Telecommunication Industry Association / Electronic Industries Alliance) предолжила группу стандартов cdma2000 (IS-2000) которые являются развитием ныне действующего IS-95. Основные отличия cdma2000 от своего предшественника — большее количество диапазонов для использования в организации мобильной связи и увеличение скорости передачи данных до 1Mbps на физическом уровне. Также добавлены новые протоколы для обеспечения всевозможных сервисов. Особо следует подчеркнуть требование стандарта об обратной совместимости с IS-95. Все мобильные станции cdma2000 должны работать в сетях IS-95, и соответственно все базовые станции cdma2000 должны обслуживать мобильные станции IS-95. Более того, имеется требование обеспечения handoff (перехода от одной соты к другой) между cdma2000 и IS-95. Таким образом, возможна незаметная для пользователя миграция сети от IS-95 к cdma2000. Также примечателен факт, что стандартом предусмотрено использование некоторых диапазонов используемых ныне старыми аналоговыми стандартами (например Band Class 5 (NMT-450)) что даёт возможность операторам этих стандартов перейти от 1-го поколения сразу к 3-ему, постепенно отдавая участки своего диапазона под cdma2000, по мере увеличения количества абонентов пользующихся новым оборудованием. Однако даже в cdma2000 сохранена возможность работы мобильных и базовых станций в аналоговом режиме. Этот режим практически идентичен стандарту AMPS с A-Key идентификацией и предназначен для обеспечения связи там, где использование цифрового режима по тем или иным причинам невозможно.

CDMA2000 был принят в группу IMT-2000, которая определяет глобальное виденье организацией ITU (International Telecommunication Union) систем 3-го поколения, в качестве одного из основных радиоинтерфейсов.

Глава 10. Сети 3G

10.1. Сеть на базе стека H.323

Серия рекомендаций H.32x предназначена для организации видеоконференций по различным типам сетей передачи данных (табл. 10.1).

Таблица 10.1

Сводная таблица протоколов семейства H.32x

Рекомендация	**H.320**	**H.321**	**H.322**	**H.323**	**H.324**
Год принятия	1990	1995	1995	1996	1996
Сеть	Узкополосная ISDN	Широкополосная ISDN, ATM	Сеть с коммутацией пакетов и гарантированным QoS (isoEthernet)	Сеть с коммутацией пакетов и негарантированным QoS (Ethernet)	Аналоговые телефонные сети (PSTN или POTS)
Видео	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263 H.264/AVC	H.261 H.263
Аудио	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.723.1 G.726 G.728 G.729	G.723
Мультиплексирование	H.221	H.221	H.221	H.225.0	H.223
Управление	H.230 H.242	H.242	H.242 H.230	H.245	H.245
Поддержка многоточечных конференций	H.231 H.243	H.231 H.243	H.231 H.243	H.323	-
Обмен данными	T.120	T.120	T.120	T.120	T.120
Сетевой интерфейс	I.400	AAL I.363 AJM I.361 PHY I.400	I.400 & TCP/IP	TCP/IP	V.34 модем

H.323 — это рекомендации ITU-T [16] для мультимедийных приложений в вычислительных сетях, не обеспечивающих гарантированное качество обслуживания (QoS). Такие сети включают в себя сети пакетной коммутации IP и IPX на базе Ethernet, Fast Ethernet и пр. Рекомендация H.323 регламентирует технические требования к коммутации речи, видео и данных по пакетным сетям, а также к связи с сетями с коммутацией каналов.

10.1.1. Архитектура сети H.323

Архитектура сети H.323 представлена на рис. 10.1.

Объектами сети H.323 являются:

- *терминал (Terminal)* — оконечное мультимедийное устройство, обеспечивающее возможность двусторонней коммуникации речи, видео или данных с другим объектом сети в реальном времени;
- *межсетевой шлюз (Gateway)* — устройство, предназначенное для преобразования мультимедийной и управляющей информации при сопряжении разнородных сетей;
- *устройство управления многоточечными соединениями (Multipoint Control Unit, MCU)* — предназначено для организации конференций с участием трёх и более участников;
- *контроллер зоны (Gatekeeper)* — рекомендуемое, но не обязательное устройство, обеспечивающее сетевое управление и исполняющее роль виртуальной телефонной станции;
- *разграничитель (Border Element)* — элемент сети H.323, посредством которого выполняется коммуникация между административными доменами.

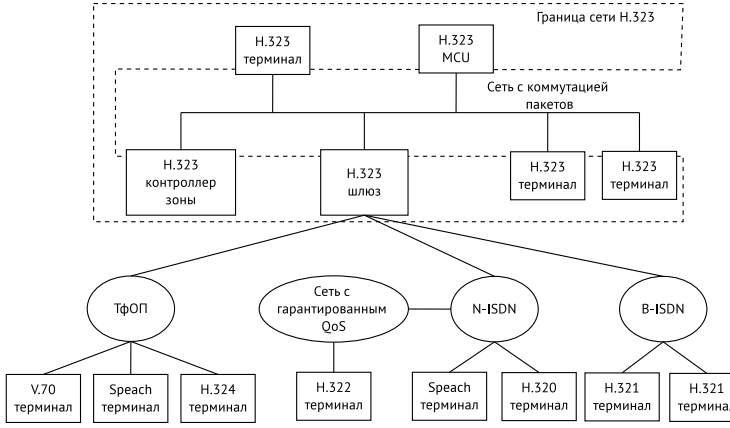

Рис. 10.1. Архитектура сети H.323

Терминал H.323 обеспечивает звуковую связь и может дополнительно поддерживать передачу видео или данных. Терминал H.323 может быть реализован как программное приложение на персональном компьютере или как самостоятельное устройство (например, телефон).

Терминал должен поддерживать следующие протоколы:

- H.245 для согласования параметров соединения;
- Q.931 для установления соединения и согласования параметров этого соединения;
- RAS (Registration/Admission/Status) для взаимодействия с контроллером зоны;
- RTP/RTCP для работы с потоками аудио и видеопакетов;
- семейство протоколов H.450;
- аудиокодек G.711 для сжатия аудиопотока.

Дополнительно терминал может поддерживать другие аудиокодеки, а также видеокодеки H.261 и/или H.263. Необязательной является поддержка протокола совместной работы над документами T.120.

Межсетевой шлюз не является обязательным компонентом сети H.323 и используется только в том случае, когда требуется установить соединение с терминалом, расположенным в сети другого типа (стандарта). Связь обеспечивается трансляцией протоколов установки и разрыва соединений, а также форматов передачи данных. Основной функцией межсетевого шлюза H.323 является преобразование сигнализационных протоколов, способа передачи, процедур коммуникации и способа кодирования, что обеспечивает возможность взаимодействия пользователей разных технологий. Шлюзы H.323 широко применяются в IP-телефонии для сопряжения IP-сетей и цифровых или аналоговых коммутируемых телефонных сетей (ISDN (Integrated Services Digital Network) или PSTN (Public Switched Telephone Network)).

Межсетевой шлюз может выполнять следующие функции:

- функция PSTN-терминала — содержит PSTN сигнализационный интерфейс, которым заканчивается PSTN сигнализация, и PSTN медиаинтерфейс, которым заканчивается медиапоток;
- функция H.323-терминала — содержит VoIP сигнализационный интерфейс, которым заканчивается H.323 сигнализация (H.225, H.245), и интерфейс пакетной передачи, которым заканчивается медиапоток, передаваемый пакетами протокола RTP;
- преобразование сигнализационных протоколов, используемых в H.323 и PSTNсетях;
- преобразование медиапотоков, сформированных при помощи различных алгоритмов сжатия;
- управление связью — координирование сигнализационных потоков и преобразование медиапотоков, в том числе и установление, изменение и разъединение соединения между медиапотоками в PSTN и IP-сети в течение вызова.

Контроллер зоны также не является обязательным компонентом сети H.323, и если используется, то обеспечивает сетевое управление и выполняет функции виртуальной телефонной станции. В этом случае контроллер зо-

ны становится центральной точкой для всех обращений внутри одной зоны — совокупности терминалов, шлюзов и серверов MCU, управляемых одним контроллером.

Контроллер зоны выполняет следующие функции:

- основные:
  - трансляция адресов — преобразование внутренних адресов сети и телефонных номеров формата E.164 (применяются в сетях ISDN) в транспортные адреса протоколов IP или IPX;
  - управление доступом — авторизация доступа в H.323-сеть путём обмена RAS-сообщениями «запрос регистрации» (ARQ), «удовлетворение запроса» (ACF) и «отклонение запроса» (ARJ);
  - управление полосой пропускания — используются RAS-сообщения «запрос ширины полосы пропускания» (BRQ), «удовлетворение запроса» (BCF) и «отклонение запроса» (BRJ);
  - управление зоной H.323 — установление вызова, использование ресурсов разрешается исключительно тем объектам сети H.323, которые зарегистрированы как члены зоны определённого контроллера зоны;
- дополнительные:
  - управление процессом установления соединений — обработка служебных сообщений протокола сигнализации Q.931 [15];
  - авторизация соединения;
  - управление вызовами — контроль за состоянием всех активных соединений, что позволяет обеспечить выделение необходимой полосы пропускания и баланс загрузки сетевых ресурсов за счёт переадресации вызовов на другие терминалы и шлюзы;
  - тарификация — хранение и обработка информации о вызовах и предоставленных услугах.

Устройство MCU предназначено для поддержки конференции между тремя и более участниками. В этом устройстве должен присутствовать *контроллер Multipoint Controller (MC)* и, возможно, *процессоры Multipoint Processors (MP)*. Контроллер MC поддерживает протокол H.245 [17] и предназначен для согласования параметров обработки аудио- и видеопотоков между терминалами. Процессоры занимаются коммутированием, микшированием и обработкой этих потоков.

Стандарт H.323 определяет три типа конференцсвязи между тремя или более числом терминалов и межсетевых шлюзов: *централизованная*, *децентрализованная*, *гибридная*.

Централизованная многоточечная конференция требует наличия устройства MCU. Каждый терминал обменивается с MCU потоками аудио, видео, данными и командами управления по схеме «точка–точка». Контроллер MC, используя протокол H.245, определяет возможности каждого терминала. Процессор MP формирует необходимые для каждого терминала мультимедийные потоки и рассылает их. Кроме того, процессор может обеспечивать преобразования потоков от различных кодеков с различными скоростями данных.

Децентрализованная многоточечная конференция использует технологию

групповой адресации. Участвующие в конференции H.323 терминалы осуществляют многоадресную передачу мультимедиа потока остальным участникам без посылки на MCU. Передача контрольной и управляющей информации осуществляется по схеме «точка–точка» между терминалами и MCU. В этом случае контроль многоточечной рассылки осуществляется контроллером MC.

Гибридная схема организации конференцсвязи является комбинацией двух
предыдущих. Участвующие в конференции H.323 терминалы осуществляют многоадресную передачу только аудио- или только видеопотока остальным участникам без посылки на MCU. Передача остальных потоков осуществляется по схеме «точка–точка» между терминалами и MCU. В этом случае задействуются как контроллер, так и процессор MCU.

10.1.2. Адресация элементов сети H.323

Адресация терминалов VoIP в основном основывается на буквенноцифровых последовательностях, распознаваемость которых обеспечена иерархической организацией группы серверов. Однако из-за потребности интеграции услуг между сетями PSTN и VoIP каждому абоненту PSTN должна быть обеспечена возможность адресации VoIP абонента, и наоборот.

Стандарт H.323 поддерживает следующие типы адресов:

- dialedDigits (в старых версиях E.164) — цифровой идентификатор в виде телефонного номера;
- h323-ID — имя пользователя или адрес электронной почты (e-mail address);
- url-ID — общий тип адреса (включает H.323-URL и PSTN-URL);
- transport-ID — транспортный адрес оконечного оборудования;
- email-ID — адрес электронной почты;
- partyNumber — цифровой идентификатор;
- mobile-UIM — идентификатор мобильных пользователей с возможностью взаимодействия с мобильными сетями общего пользования 2G и 3G.

Такой подход требует отдельного преобразования и распознавания адреса, а также особых процедур регистрации, обеспечиваемых контроллерами зоны H.323 и разграничителями.

В случае адресации с помощью цифр телефонного номера используются префикс зоны и технологический префикс, однозначно определяющие зону административного домена.

Каждое устройство в сети H.323 может иметь более одного адреса (возможно, одного и того же типа). Единственное условие — все адреса одного устройства должны ссылаться на уникальный транспортный адрес этого устройства.

10.1.3. Основные характеристики H.323

Основные характеристики H.323:
- независимость от сети — возможна работа поверх существующих архитектур сетей;
- управление шириной полосы — каждому H.323-вызову выделяется определённая ширина полосы;
- независимость от приложения и платформы — не требуется применения определённой аппаратной или программной платформы;
- поддержка многосторонних конференций;
- взаимодействие — прозрачная коммутация для конечного пользователя;
- гибкость — в одной H.323 конференции могут участвовать терминалы различных возможностей коммуникации.

10.1.4. Обработка звуковых сигналов (Audio Signal)

Одним из важных факторов эффективного использования пропускной способности IP-канала является выбор оптимального алгоритма кодирования / декодирования речевой информации — кодека.

Типы речевых кодеков по принципу действия можно разделить на три группы:
1. кодеки с импульсно-кодовой модуляцией (ИКМ) и адаптивной дифференциальной импульсно-кодовой модуляцией (АДИКМ):
   - разработаны в конце 1950-х годов,
   - используются в системах традиционной телефонии;
2. кодеки с вокодерным[1] преобразованием речевого сигнала:
   - разработаны для снижения требований к пропускной способности радиотракта в системах мобильной связи,
   - применяется гармонический синтез сигнала на основании информации о его вокальных составляющих — фонемах,
   - реализованы как аналоговые устройства;
3. комбинированные (гибридные) кодеки:
   - сочетают в себе технологию вокодерного преобразования / синтеза речи, но оперируют с цифровым сигналом посредством специализированных преобразователей цифровых сигналов,
   - содержат в себе ИКМ или АДИКМ кодек и реализованный цифровым способом вокодер.

[1] Вокодер — электронный цифровой музыкальный инструмент, преобразующий звук человеческого голоса путём изменения его волновых и частотных характеристик.

10.1.4.1. Оценка MOS

MOS (Mean Opinion Score) — средняя экспертная оценка разборчивости речи — метод субъективного тестирования качества речи, часто используемый для сравнения характеристик речевых кодеков, при котором слушатели выставляют оценки по пятибалльной системе. Результирующая оценка MOS вычисляется как среднее арифметическое для большого числа оценок.

Таблица 10.2

Оценки MOS

Качество	Оценка MOS
высокое	$4,0$–$5,0$
стандартное телефонное	$3,5$–$4,0$
приемлемое	$3,0$–$3,5$
синтезированный звук	$2,5$–$3,0$

10.1.4.2. G.711

Рекомендация G.711 [18] описывает кодек, использующий преобразование аналогового сигнала с точностью 8 бит, тактовой частотой 8 КГц и простейшей компрессией амплитуды сигнала. Скорость потока данных на выходе преобразователя составляет 64 Кбит/с (8 бит x 8 КГц). Для снижения шума квантования и улучшения преобразования сигналов с небольшой амплитудой при кодировании используется нелинейное квантование по уровню согласно специальному псевдологарифмическому закону. Существуют два основных алгоритма, представленных в стандарте:

1. μ-law (используется в Северной Америке и Японии):
   прямое преобразование:

$$F(x) = \operatorname{sgn}(x)\frac{\ln(1+\mu|x|)}{\ln(1+\mu)}, \quad -1 \leqslant x \leqslant 1;$$

   обратное преобразование:

$$F^{-1}(y) = \operatorname{sgn}(y)\frac{1}{\mu}\left[(1+\mu)^{|y|}-1\right], \quad -1 \leqslant y \leqslant 1,$$

   где $\mu = 255$ (8 бит).
2. A-law (используется в Европе и в остальном мире):

прямое преобразование:

$$F(x) = \operatorname{sgn}(x) \begin{cases} A\dfrac{|x|}{1+\ln(A)}, & |x| \leqslant \dfrac{1}{A}, \\ \dfrac{1+\ln(A|x|)}{1+\ln(A)}, & \dfrac{1}{A} \leqslant |x| \leqslant 1; \end{cases}$$

обратное преобразование:

$$F^{-1}(y) = \operatorname{sgn}(y) \begin{cases} \dfrac{|y|(1+\ln(A))}{A}, & |y| \leqslant \dfrac{1}{1+\ln(A)}, \\ \dfrac{\exp(|y|(1+\ln(A))-1)}{A}, & \dfrac{1}{1+\ln(A)} \leqslant |y| < 1, \end{cases}$$

где $A = 87,6$ — параметр сжатия.

Оба алгоритма являются логарифмическими, но более поздний A-law был изначально предназначен для компьютерной обработки процессов.

Типичная оценка MOS составляет $4,2$. Обычно любое устройство VoIP поддерживает этот тип кодирования.

Кодек G.711 широко распространён в системах традиционной телефонии с коммутацией каналов. Несмотря на то, что рекомендация G.711 в стандарте H.323 является основной и первичной, в шлюзах IP-телефонии данный кодек применяется редко из-за высоких требований к полосе пропускания и задержкам в канале передачи. Использование G.711 в системах IP-телефонии обоснованно лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров.

10.1.4.3. G.723.1

Кодек G.723.1 [19] является одним из базовых кодеков сжатия речи, утверждённым ITU-T в рекомендации G.723.1 в ноябре 1995 г. Кодек предназначен для приложений IP-телефонии, в частности, для организации видеоконференций по телефонным сетям. Рекомендация G.723.1 является частью более общего стандарта H.324, описывающего подход к организации видеоконференций, при этом целью является обеспечение видеоконференций с использованием обычных модемов.

Кодек G.723.1 представляет собой комбинацию аналого-цифрового преобразования / цифро-аналогового преобразования и вокодера. Применение вокодера позволяет снизить скорость передачи данных в канале, что принципиально важно для эффективного использования как радиотракта, так и IP-канала.

Кодек G.723.1 осуществляет преобразование аналогового сигнала в поток данных со скоростью 64 Кбит/с (ИКМ), а затем при помощи многополосно-

го цифрового фильтра / вокодера выделяет частотные фонемы, анализирует их и передаёт по IP-каналу информацию только о текущем состоянии фонем в речевом сигнале. Данный алгоритм преобразования позволяет снизить скорость кодированной информации до 5, 3–6, 3 Кбит/с без видимого ухудшения качества речи.

Кодек G.723.1 предусматривает два режима работы: 6, 3 Кбит/с (кадр имеет размер 189 бит, дополненных до 24 байт) и 5, 3 Кбит/с (кадр имеет размер 158 бит, дополненных до 20 байт). Первый режим применяется для сетей с пакетной передачей голоса и использует алгоритм сжатия речи MP-MLQ (Multipulse Maximum Likelihood Quantization — многоимпульсное квантование с максимальным правдоподобием), который позволяет добиться весьма существенного сжатия речевой информации при сохранении достаточно высокого качества звучания. Второй режим применяется в сетях со смешанным типом трафика (голос / данные) и использует алгоритм CELP (Code Excited Linear Prediction — кодирование с линейным предсказанием). Режим работы кодека G.723.1 может меняться динамически от кадра к кадру.

Алгоритм CELP [20,21] построен на модели кодирования с использованием процедуры «анализа через синтез», линейного предсказания и векторного квантования. CELP-анализ состоит из трёх основных процедур:

- кратковременное линейное предсказание;
- долговременный поиск по адаптивной кодовой книге;
- поиск по стохастической кодовой книге.

CELP-синтез состоит из этих же процедур, выполненных в обратном порядке.

Кодер оперирует с кадрами речевого сигнала длиной 30 мс, дискретизованными с частотой 8 КГц. Для каждого кадра производится анализ речевого сигнала и выделяются передаваемые параметры CELP-модели: 10 линейных спектральных пар (несут информацию о коэффициентах фильтра линейного предсказания), индексы и коэффициенты усиления в адаптивной и фиксированной кодовых книгах. Далее эти параметры кодируются в битовый поток и передаются в канал.

В декодере эта битовая посылка используется для восстановления параметров сигнала возбуждения и коэффициентов синтезирующего фильтра. Далее восстанавливается речь путём пропускания сигнала возбуждения через синтезирующий фильтр. Затем для улучшения качества восприятия синтетического сигнала выходной сигнал с фильтра-синтезатора пропускается через постфильтр.

Длительность кадров кодека G.723.1 составляет 30 мс с длительностью предварительного анализа сигнала 7, 5 мс.

Оценка MOS для данного кодека составляет 3, 9 в режиме 6, 3 Кбит/с и 3, 7 — в режиме 5, 3 Кбит/с.

10.1.4.4. Кодек G.726

Рекомендация G.726 основана на алгоритме кодирования ADPCM — адаптивная дифференциальная ИКМ. Этот алгоритм даёт практически такое

же качество воспроизведения речи, как и ИКМ, однако для передачи информации при его использовании требуется полоса всего 16–32 Кбит/с. Кодек предназначен для использования в системах видеоконференций; в приложениях IP-телефонии этот кодек практически не применяется. Оценка по MOS составляет $4,3$.

10.1.4.5. G.728

Алгоритм G.728 стандартизован ITU в 1992 г. [22], основан на методе LD-CELP (Low-Delay Code Excited Linear Prediction — кодирование с линейным предсказанием и низкой задержкой) и предназначен для сжатия и передачи речевых данных со скоростью 16 Кбит/с, при этом внося задержку при кодировании от 3 до 5 мс.

Алгоритм применяется к цифровой последовательности, получаемой в результате аналого-цифрового преобразования речевого сигнала с 16-разрядным разрешением. Входной сигнал с частотой дискретизации 8кГц, сжатый по A- или μ-закону (см. раздел 10.1.4.2), преобразуется для получения линейного кода.

Оценка MOS для данного кодека составляет $3,6$.

Предназначен для использования в основном в системах видеоконференций. В устройствах IP-телефонии данный кодек применяется достаточно редко.

10.1.4.6. G.729

В основе кодеков G.729 [23–25] лежит алгоритм CS-ACELP (Conjugate Structure – Algebraic Code Excited Linear Prediction) — сопряжённая структура с управляемым алгебраическим кодированием с линейным предсказанием. Процесс преобразования вносит задержку 15 мс. Скорость кодированного речевого сигнала составляет 8 Кбит/с.

Алгоритм основан на модели кодирования с использованием линейного предсказания по алгебраической кодовой книге (CELP-модель). Кодер оперирует с кадрами речевого сигнала длительностью 10 мс, дискретизованными с частотой 8КГц, что соответствует 80 16-битным отсчётам в линейном законе. Для каждого кадра производится анализ речевого сигнала и выделяются параметры модели (коэффициенты фильтра линейного предсказания, индексы и коэффициенты усиления в адаптивной и фиксированной кодовых книгах). Далее эти параметры кодируются и передаются в канал.

В декодере битовая посылка используется для восстановления параметров сигнала возбуждения и коэффициентов синтезирующего фильтра. Речь восстанавливается путём пропускания сигнала через кратковременный синтезирующий фильтр.

Синтезирующий фильтр имеет полюсную передаточную функцию 10-го порядка. Для работы синтезатора основного тона используется адаптивная кодовая книга. В последующем речь улучшается адаптивной постфильтрацией.

В случае потери передаваемой кодером битовой посылки исходные данные для речевого синтезатора получаются интерполяцией данных с предыдущих не повреждённых кадров, но при этом энергия интерполированного речевого сигнала постепенно уменьшается, что не создаёт особого дискомфорта у слушателя.

В устройствах VoIP и VoFR данный кодек занимает лидирующее положение, обеспечивая наилучшее качество кодирования речевой информации при достаточно высокой компрессии.

10.1.5. Обработка видеосигналов (Video Signal)

Стандарт H.323 [16] устанавливает два формата изображения — CIF (352×288 пиксела) для яркостного сигнала и QCIF (176×144 пиксела), т.е. с $1/4$ частью разрешения CIF, причём частота смены кадров не должна опускаться ниже 24 кадров в секунду.

CIF (Common Itermediate Format — общий формат обмена) представляет собой стандарт видеоизображения с размером кадра 352×288 пиксела и частотой кадров $7,5$, 10, 15 или 30 к/с. Цвет кодируется в формате YUV (представление цвета, при котором каждый элемент изображения представляется тремя компонентами: яркостной и двумя цветоразностными) с разрядностью 8 бит. Производные форматы: QCIF — 176×144 пикселов, subQCIF — 128×96 пикселов, 4CIF — 704×576 пикселов, 16CIF — 1408×1152 пикселов.

Для компрессии/декомпрессии видеосигнала используются кодеки H.261, H.263, H.264. Различаются они способом обработки изображения.

10.1.5.1. H.261

Стандарт H.261 [26] определяет видеокодек H.261 для аудиовизуальных услуг со скоростью $P \times 64$ Кбит/с, где P может меняться в диапазоне от 1 до 30. В данном кодеке реализована комбинация алгоритмов *DCT (Discrete Cosine Transform)* и *Motion Prediction*.

Алгоритм *DCT (Discrete Cosine Transform — дискретное косинуспреобразование, ДКП)* разработан в 1981 г. В [27,28] даётся следующее определение.

Определение. Пусть дано изображение размером $N \times N$. Тогда прямое ДКП записывается в виде:

$$t(u,v) = c(u)c(v) \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} I(k,l) \cos \frac{(2k+1)u\pi}{2N} \cos \frac{(2l+1)v\pi}{2N},$$

$$c(m) = \begin{cases} \sqrt{\frac{1}{N}}, m = 0, \\ \sqrt{\frac{2}{N}}, m \neq 0, \end{cases} \qquad u, v = \overline{1, N-1},$$

а обратное:

$$I(k,l) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} t(u,v)c(u)c(v)\cos\frac{(2k+1)u\pi}{2N}\cos\frac{(2l+1)v\pi}{2N},$$

$$c(m) = \begin{cases} \sqrt{\frac{1}{N}}, & m = 0, \\ \sqrt{\frac{2}{N}}, & m \neq 0. \end{cases} \qquad k,l = \overline{1,N-1},$$

Здесь коэффициенты $t(u,v)$ — амплитуды пространственных частот изображения.

Дискретное преобразование обладает следующими свойствами:

- некоррелированность коэффициентов — коэффициенты независимы друг от друга, т.е. точность представления одного коэффициента не зависит от любого другого;
- «уплотнение» энергии — преобразование сохраняет основную информацию в малом количестве коэффициентов.

Motion Prediction — предсказание перемещения — техника межкадрового кодирования, применяемая в кодеках для сжатия сигнала движущегося изображения. В последовательности кадров каждый пиксель в текущем кадре перемещён по сравнению с предшествующим кадром. При этом соседние пиксели перемещаются практически одинаково. Кадр делится на блоки пикселей (16×16 или 8×8), и для описания движения пикселей всего блока вычисляется вектор оценки перемещения (*Motion Estimation*). Предсказание перемещения текущего блока, полученное из предшествующего кадра с помощью вектора компенсации перемещения (*Motion Compensation*), сравнивается с настоящим текущим блоком и формируется, если надо, ошибка предсказания (т.е. компенсация неточности предсказания). Для таких блоков передаётся только вектор оценки перемещения и ошибка предсказания, что значительно экономней простой передачи содержимого блока.

10.1.5.2. H.263

Стандарт H.263 [29] разработан в 1995 г. и определяет видеокодек H.263, предназначенный для передачи видеоизображения с малой скоростью (ниже 64 Кбит/с, например, для связи с помощью модема и аналоговых телефонных линий). Кодек H.263 использует технологию H.261 с дополнительными усовершенствованиями, главным образом в области предсказания перемещения. В отличие от H.261, для которого предсказываемые направления должны лежать в пределах изображения, для H.263 они могут выходить за границы изображения. Это особенно важно при низких скоростях передачи, не являющихся обязательными для стандарта H.261. Кроме того, кодек H.263 позволяет загружать канал связи практически только изменениями картинки.

Дальнейшим развитием проекта являются кодеки H.263v2 (также известный как H.263+ или H.263 1998) и H.263v3 (известный как H.263++ или H.263 2000).

10.1.5.3. H.264

Стандарт H.264 [30] разработан совместно ITU-T и MPEG и является развитием H.263. Он определяет одноимённый кодек H.264, также известный как *AVC (Advanced Video Coding)* и *MPEG-4* [31], который имеет существенно расширенные возможности по сравнению с H.263, вследствие чего стал основным при разработке программного обеспечения для видеоконференций.

Основные характеристики H.264:

- Многокадровое предсказание перемещения кадров:
  - Более гибкое использование сжатых ранее кадров в качестве опорных. Разрешается использование до 32 ссылок на другие кадры, что поднимает эффективность кодирования, так как позволяет кодеру выбирать для компенсации движения между большим количеством изображений.
  - Независимость порядка воспроизведения изображений и порядка опорных изображений, что позволяет кодеру выбирать порядок изображений для компенсации движения и для воспроизведения с высокой степенью гибкости, которая ограничена только объёмом памяти, гарантирующим возможность декодирования. Устранение ограничения также позволяет в ряде случаев устранить дополнительную задержку, ранее связанную с двунаправленным предсказанием.
  - Независимость методов обработки изображений и возможности их использования для предсказания движения, что обеспечивает кодеру большую гибкость и возможность использовать для предсказания движения изображение, более близкое по содержанию к кодируемому.
  - Компенсация движения с переменным размером блока (от 16×16 до 4×4 пикселя) позволяет крайне точно выделять области движения.
  - Вектора движения, выводящие за границы изображения (по аналогии с H.263).
  - Шеститочечная фильтрация компонента яркости для полупиксельного предсказания с целью уменьшения зубчатости краёв и обеспечения большей чёткости изображения.
  - Точность до четверти пиксела при компенсации движения обеспечивает очень высокую точность описания движущихся областей (что особенно актуально для медленного движения).
  - Взвешенное предсказание, позволяющее использовать масштабирование и сдвиг после компенсации движения на величины, указанные кодером. Такая методика может чрезвычайно сильно поднять эффективность кодирования для сцен с изменением освещённости, например, при эффектах затемнения, постепенного появления изображения.
- Пространственное предсказание от краёв соседних блоков для I-кадров (от англ. Intra Pictures). Новая методика экстраполяции краёв ранее декодиро-

ванных частей текущего изображения повышает качество сигнала, используемого для предсказания.
- Сжатие макроблоков без потерь:
  - Метод представления макроблоков без потерь в ИКМ, при котором видеоданные представлены непосредственно, что позволяет точно описывать определённые области и допускать строгое ограничение на количество закодированных данных для каждого макроблока.
  - Улучшенный метод представления макроблоков без потерь, позволяющий точно описывать определённые области, затрачивая при этом существенно меньше битов, чем ИКМ.
- Гибкие функции чересстрочного сжатия:
  - Адаптивное к изображению кодирование полей (PAFF), позволяющее кодировать каждый кадр как кадр или как пару полей (полукадров) — в зависимости от отсутствия/наличия движения.
  - Адаптивное к макроблокам кодирование полей (MBAFF), позволяющее независимо кодировать каждую вертикальную пару макроблоков (блок 16×32) как прогрессивные или чересстрочные. Позволяет использовать макроблоки 16×16 в режиме разбиения на поля.
- Новые функции преобразования:
  - Точное целочисленное преобразование пространственных блоков 4×4, позволяющее точно разместить разностные сигналы с минимумом шума.
  - Точное целочисленное преобразование пространственных блоков 8×8, обеспечивающее большую эффективность сжатия схожих областей, чем 4×4.
  - Адаптивный выбор кодеком между размерами блока 4×4 и 8×8.
- Дополнительное преобразование Адамара (разложение обрабатываемых сигналов по системе прямоугольных базисных функций), применяемое к дискретнокосинусным коэффициентам основного пространственного преобразования (к коэффициентам яркости и, в особом случае, цветности) для достижения большей степени сжатия в однородных областях.
- Квантование:
  - Логарифмическое управление длиной шага для упрощения распределения битрейта (битовая скорость передачи данных) кодером и упрощённого вычисления обратной функции квантования.
  - Частотно-оптимизированные матрицы масштабирования квантования, выбираемые кодером для оптимизации квантования на основе человеческих особенностей восприятия.
- Внутренний фильтр деблокинга (удаление блочности) в цикле кодирования, устраняющий артефакты (искажение) блочности, часто возникающие при использовании основанных на DCTтехниках сжатия изображений.
- Энтропийное кодирование[1] квантованных коэффициентов трансформации:

[1] *Энтропийное кодирование* — кодирование словами (кодами) переменной длины, при которой длина кода символа имеет обратную зависимость от вероятности появления символа в

  - *Context-adaptive binary arithmetic coding (CABAC) — контекстнозависимое адаптивное бинарное арифметическое кодирование* — алгоритм сжатия без потерь синтаксических элементов видеопотока на основе вероятности их появления.
  - *Context-adaptive variable-length coding (CAVLC) — контекстнозависимое адаптивное кодирование с переменной длиной кодового слова* — альтернатива CABAC меньшей сложности.
  - Часто используемое, простое и высокоструктурированное кодирование словами переменной длины многих элементов синтаксиса, не закодированных CABAC или CAVLC, известное как Exp-Golomb (экспоненциальное кодирование Голомба).
- Функции устойчивости к ошибкам:
  - Определение уровня сетевой абстракции, позволяющее использовать один и тот же синтаксис видео в различных сетевых окружениях, включая наборы параметров последовательности и наборы параметров изображения, которые обеспечивают большую надёжность и гибкость, чем предыдущие технологии.
  - Гибкое упорядочивание макроблоков, также известное как группы частей и произвольное упорядочивание частей — методы реструктурирования порядка представления макроблоков в изображениях.
- Благодаря произвольному упорядочиванию частей новый стандарт позволяет посылать и получать их в произвольном порядке друг относительно друга. Это может снизить задержку в приложениях реального времени.
  - Разбиение данных — функция, обеспечивающая разделение данных разной важности по разным пакетам данных с разными уровнями защиты от ошибок.
  - Избыточные части. Возможность посылки кодером избыточного представления областей изображений, позволяя воспроизвести области изображений, данные о которых были потеряны в процессе передачи.
  - Нумерация кадров, позволяющая создать «подпоследовательности» (включая временное масштабирование включением дополнительных кадров между другими), а также обнаружить (и скрыть) потери целых кадров при сбоях канала или пропаже пакетов.

10.1.6. Конференц-связь для передачи данных (Data)

Стандарт T.120 [32] представляет собой совокупность телекоммуникационных и прикладных протоколов для организации и проведения многоточечной конференции в реальном времени [33].

Данный стандарт регламентирует порядок организации и поддержания конференций на любой платформе, управление множеством участников и программ, безошибочный и безопасный обмен данными при различных возможных сетевых сценариях.

передаваемом сообщении.

В семейство T.120 входят следующие протоколы:

- T.121 представляет основу для разработки прикладных протоколов;
- T.122 совместно с T.125 определяет доступные многоточечные услуги;
- T.123 специфицирует транспортные профили ТфОП, ISDN, цифровых сетей с коммутацией каналов CSDN, цифровых сетей с коммутацией пакетов PSDN, сети Novell NetWare IPX и сети TCP/IP; обеспечивает вышележащим уровням независимость от типа сети и предоставляет четыре канала разного приоритета между двумя точками, что необходимо для обеспечения преимущества пересылки данных реального времени (например, информации о перемещении курсора) перед фоновой передачей данных (например, транспортировкой файлов);
- T.124 регламентирует общий процесс управления конференцией Generic Conference Control (GCC), обеспечивая полный набор инструментов для её организации и управления; в частности, GCC обеспечивает функции ведущего конференции и функции резервирования.
- T.125 описывает многоточечный протокол связи (Multipoint Communication Service Protocol, MCS), задающий процедуры для передачи сигнальной информации и данных между провайдерами MCS; при многоточечном соединении можно ограничить доступ к определённым наборам данных, сделав их доступными лишь для некоторых участников телеконференции;
- T.126 определяет процедуры просмотра и аннотирования неподвижных изображений между двумя или несколькими приложениями;
- T.127 предусматривает средства файлового обмена между участниками конференции, в том числе их одновременную приоритетную передачу, а также опции для сжатия файлов перед их транспортированием;
- T.128 регламентирует аудиовизуальное управление.

Стек протоколов T.120 имеет двухуровневую архитектуру. Протоколы T.122, T.123, T.124 и T.125 образуют нижний уровень и описывают независимый от приложений механизм для организации многоточечной связи. В тоже время, протоколы T.126, T.127 и T.128 располагаются на верхнем уровне и по своей сути являются прикладными протоколами. Следует отметить, что в рамках одной конференции могут сосуществовать как стандартизованные, так и нестандартизованные приложения.

В зависимости от конкретной реализации продукты T.120 могут устанавливать соединения, выполнять передачу и приём данных и работать совместно, используя программное разделение, передачу файлов и др.

10.1.7. Управление (Control)

Совокупная система управления H.323 основывается на трёх отдельных сигнализационных каналах: канале H.245, канале установления вызова и RASканале.

Протокол управления мультимедийной конференцией H.245 [17] обеспечивает согласование возможностей компонентов, установление и разрыв ло-

гических соединений, передачу запросов на установление приоритета, управление потоком (загрузкой канала), передачу общих команд и индикаторов.

Сообщения протокола H.245 передаются по H.245-каналу управления, используя коммутируемый способ передачи данных с помощью протокола TCP, что гарантирует последовательную передачу данных без ошибок. Между любыми двумя элементами сети можно установить только один H.245канал.

Межтерминальный обмен параметрами позволяет согласовывать режимы работы и форматы кодирования информации, что обеспечивает взаимодействие терминалов от разных производителей. В процессе обмена сообщениями о параметрах уточняются возможности терминалов по приёму и передаче различных видов трафика.

Все H.245сигнализационные сообщения принадлежат одной из следующих категорий:

- запрос (Request) — сообщения, которые требуют от получателя выполнения определённых действий, включая и ответ на принятый запрос;
- ответ (Response) — сообщения, которые посылаются в ответ на сообщения из предыдущей категории;
- команда (Command) — команды, которые от получателя требуют выполнения определённых действий, но не включают ответ на команду;
- индикация (Indication) — сообщения информативного типа, которые от получателя не требуют ни действий, ни ответа.

Процедуры H.245:

- объявление о возможности обмена медиа потоками (Capabilities Exchange) — информация, необходимая для выбора поддерживаемого обеими сторонами вида медиа коммуникации;
- определение ведущей стороны в коммуникации (Master Slave Determination) — договорённость о ведущем и ведомых оконечных узлах;
- открытие и закрытие логических каналов сигнализации (Logical Channel Signalling);
- запрос на изменение установленного соединения (Request Mode) — запрос на изменение характеристик медиа потока;
- закрытие канала H.245.

Если канал установления вызова ненадёжный, то для обмена сигнализацией применяется протокол H.225.0 [34], используя некоммутируемый способ передачи данных с помощью протокола UDP. В этом случае для установления вызова определён отдельный механизм подтверждения приёма и повторной передачи, т.к. для сигнализации, связанной с установлением вызова, требуется надёжная передача.

Протокол H.225.0 представляет собой протокол сигнализации для установления и разъединения H.323 вызова между двумя H.323 оконечными точками. В рамках этого протокола определена и процедура ускоренного соединения (Fast Connect Procedure).

Протокол H.225.0 в рамках процедур, требуемых для установления и разъединения вызова, определяет использование следующих сообщений:

- Setup — сообщение о начале установления соединения;
- Setup Acknowledge — подтверждение установления соединения;

- Information — информация, необходимая для установления вызова, или другие сведения, относящиеся к вызову;
- Call Proceeding — сообщение о продолжении установления вызова;
- Progress — в этом сообщении посылается информация о дальнейшем развитии вызова при взаимодействии с сетями с коммутацией каналов;
- Alerting — оповещение о входящем вызове;
- Connect — сообщение об установлении соединения;
- Facility — сообщение для осуществления дополнительных услуг и туннелирования H.245сообщений по каналам установления вызова;
- Status Inquiry — запрос статуса вызова;
- Status — сообщение содержит статус вызова из аспекта отправителя сообщения и причину его передачи;
- Notify — уведомление, содержащее информацию о вызове, например, индикацию временного прерывания (user suspend) или возобновления (user resume) вызова;
- Release Complete — полное разъединение вызова.

Протокол сигнализации RAS (Registration, Admission and Status — регистрация, подтверждение и статус) применяется для передачи служебных сообщений между терминалами и контроллером зоны. RAS-сообщения служат для регистрации терминалов, допуска их к сеансу связи, изменения используемой полосы пропускания, информирования о состоянии сеанса и его прекращении. В отсутствие контроллера зоны протокол RAS не используется.

Основные процедуры в рамках протокола RAS:

- обнаружение контроллера зоны;
- регистрация оконечного узла (терминала);
- управление доступом;
- управление шириной полосы пропускания;
- определение местонахождения оконечного узла;
- получения подробной статусной информации о вызовах.

Оконечные узлы используют протокол RAS для обнаружения контроллеров зоны, регистрации, а затем для получения разрешения на право использования части ресурсов системы, а также для получения транспортных адресов других удалённых оконечных узлов. Контроллеры зоны, в свою очередь, посредством процедур регистрации и одобрения доступа используют протокол RAS для управления своей зоной, надзора за статусом регистрированных оконечных узлов, управления шириной полосы пропускания и определения местоположения оконечных узлов в других зонах посредством обмена адресной информацией с их контроллерами зоны.

10.1.8. Мультимедийная передача.

Протокол RTP (RFC 1889) обеспечивает в IP-сетях доставку адресатам аудио- и видеопотоков в масштабе реального времени. RTP идентифицирует тип и номер пакета, устанавливает в него метку синхронизации. На основе этой информации приёмный терминал синхронизирует звук, видео и

данные, осуществляет их последовательное и непрерывное воспроизведение. Корректное функционирование RTP возможно при наличии в абонентских терминалах механизмов буферизации принимаемой информации.

Транспортный протокол управления передачей в режиме реального времени RTCP (RFC 1889) контролирует реализацию функций RTP. Он также отслеживает качество обслуживания и снабжает соответствующей информацией компоненты, участвующие в конференции.

10.1.9. Эволюция H.323

Первоначально протокол H.323 был предназначен исключительно для локальных сетей и не охватывал проблемы QoS и надёжности.

Вторая версия протокола H.323 одобрена в феврале 1998 г. Были введены некоторые новые функции, связанные с технологией VoIP.

Особое внимание уделялось механизмам обеспечения надёжной H.323-коммуникации в рамках рекомендации H.235 [35]:

- подтверждение достоверности — механизм, которым подтверждается достоверность оконечных точек, участвующих в конференции;
- неприкосновенность данных — механизм контроля целостности принятых пакетных данных;
- защита персональной информации / конфиденциальность коммуникации путём кодирования и декодирования;
- невозможность отрицания — способ предотвращения возможности отрицания участия в конференции.

Другим улучшением в этой версии стало добавление процедуры ускоренного соединения (Fast Connect) — нового быстрого метода установления вызова, а также процедуры передачи сообщений H.245 по каналу установления вызова (туннелирование), вследствие чего потребность надёжных (TCP) соединений в вызове была сведена к одному соединению, что дополнительно сократило время установления вызова.

Кроме того, во второй версии H.323 были введены первые дополнительные услуги в серии рекомендаций H.450: переадресация вызова (Call Transfer) [36] и изменение маршрута вызова (Call Diversion) [37].

Вторая версия охватывает и некоторые аспекты QoS, обеспечивая оконечным точкам H.323 возможность введения параметров качества для медиа потоков.

Улучшения второй версии коснулись и контроллера зоны — была введена концепция альтернативных контроллеров зоны, на которые перенаправлялась часть запросов с основного контроллера зоны в случае высокой нагрузки или неисправности.

Третья версия была утверждена в сентябре 1999 г. В этой версии стала возможной передача сигнализации для установления большего числа вызовов посредством одного TCPсоединения, а также удержание установленного TCPсоединения при отсутствии вызова.

Дополнение E (Annex E) к рекомендации H.323 обеспечило стандарту H.323 альтернативное решение — передачу сигнализации для установления вызова по ненадёжному каналу, используя протокол UDP, что позволило уменьшить время установления вызова и улучшить управление такими параметрами, как время повторной передачи неподтверждённых сообщений и определение ошибки удалённой H.323 оконечной точки, с которой осуществлена коммуникация.

В третьей версии было разработано дополнение рекомендации H.225.0, Annex G, описывающее методы и сигнализацию, необходимую для распознавания адреса, разрешения доступа, обмена информацией о тарификации и ценах на услуги, а также регистрации использования между административными доменами. Кроме того, это дополнение ввело в архитектуру H.323 новый элемент — разграничитель (Border Element).

В четвёртую версию, принятую в ноябре 2000 г., было введено множество улучшений с целью удержания в то время передовой позиции протокола VoIP. Улучшения коснулись надёжности, наращиваемости и гибкости структуры H.323.

Протокол для взаимодействия межсетевого шлюза (Media Gateway, MG) и контроллера межсетевого шлюза (Media Gateway Controller, MGC) разработан исследовательской группой 16 организации ITU- T в сотрудничестве с организацией IETF и описан в рекомендации H.248.

Помимо того, что в четвёртой версии была расширена группа поддерживаемых дополнительных услуг, также были введены два новых механизма предоставления дополнительных услуг — механизм управления H.323-устройствами, базирующийся на протоколе HTTP, и механизм управления, базирующийся на стимулировании. Механизмы описаны в дополнениях (Annex K и L) к рекомендации H.323.

Пятая версия H.323 была одобрена в июле 2003 г. и, в отличие от предыдущих версий, была направлена на стабилизацию протокола.

10.2. Концепция Softswitch. Протокол SIP

Softswitch является носителем интеллектуальных возможностей сети, который координирует управление обслуживанием вызовов, сигнализацию и функции, обеспечивающие установление соединения через одну или несколько сетей.

Softswitch: управляет обслуживанием вызовов; координирует обмен сигнальными сообщениями между сетями.

10.2.1. Архитектура Softswitch

Архитектура Softswitch (рис. 10.2) представляет собой набор функциональных объектов (функций, а не физических объектов), соединённых между собой посредством интерфейсов.

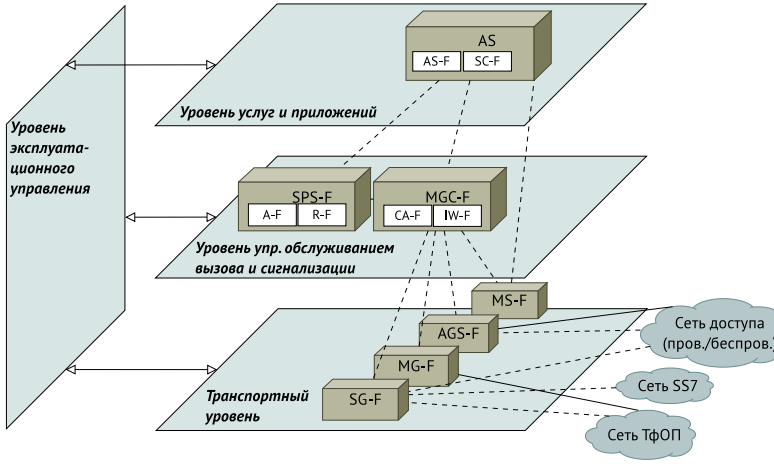

Рис. 10.2. Архитектура Softswitch (пунктирная линия — сигнализация, сплошная — данные)

В зависимости от своей функциональности функциональные объекты (ФО) распределены по функциональным уровням. Выделяют четыре функциональных уровня:

- *транспортный уровень (Transport Plane)* — отвечает за транспортировку сообщений по сети связи и обеспечивает доступ к сети IPтелефонии сигнальной и/или пользовательской информации, поступающей со стороны других сетей или терминалов;
- *уровень управления обслуживанием вызова и сигнализации (Call Control & Signaling Plane)* — управляет основными элементами сети IPтелефонии;
- *уровень услуг и приложений (Service & Application Plane)* — реализует управление услугами и/или приложениями в сети IPтелефонии, их логику и выполнение, а также управление специализированными компонентами передачи пользовательской информации (например, медиасерверами);
- *уровень эксплуатационного управления (Management Plane)* — обеспечивает выполнение функций активизации абонентов и услуг, техобслуживания, биллинга и пр.

Элементы транспортного уровня:

- *ФО шлюза сигнализации (Signaling Gateway Function, SG-F)* — обеспечивает обмен сигнальной информацией между сетью IP-телефонии и ТфОП или между транзитной пакетной IP-сетью и сетью сотовой подвижной связи с коммутацией каналов на базе стека SS7; использует протоколы Sigtran типов TUA, SUA и M3UA over SCTP;
- *ФО сигнализации шлюза доступа (Access Gateway Signaling Function, AGS-*

F) — обеспечивает обмен сигнальной информацией между сетью IPтелефонии и сетью доступа с коммутацией каналов на базе интерфейса V5.1/V5.2 или ISDN, а также между транзитной сетью подвижной связи с коммутацией пакетов и сетью сотовой подвижной связи на базе TDM или ATM; использует протоколы Sigtran типов TUA, SUA и M3UA over SCTP;

- *ФО медиашлюза (Media Gateway Function, MG-F)* — обеспечивает сопряжение IP-сети с портом доступа, с соединительной линией или с совокупностью портов и/или соединительных линий, выполняя таким образом функции шлюза между пакетной сетью и внешними сетями с коммутацией каналов, такими как ТфОП, сеть сотовой подвижной связи или ATM; использует протоколы и технологии RTP/RTCP, TDM, H. 248 и MGCP;
- *ФО медиасервера (Media Server Function, MS-F)* — обеспечивает управление обработкой пользовательского пакетного трафика от приложений; использует протоколы SIP, MGCP и H. 248.

Элементы уровня управления обслуживанием вызова и сигнализации:

- *ФО контроллера медиашлюзов (Media Gateway Controller Function, MGC-F)* — представляет собой логический элемент управления обслуживанием вызова и сигнализации для одного или более транспортных шлюзов:
  - *ФО устройства управления шлюзом (Call Agent Function, CA-F)* — обеспечивает обработку вызова и определяет состояние процесса его обслуживания; может использовать протоколы SIP, SIP-T, BICC, H. 323, Q. 931, Q. SIG, INAP, ISUP, TCAP, BSSAP, RANAP, MAP и CAP;
  - *ФО взаимодействия (Interworking Function, IW-F)* — обеспечивает взаимодействие между разными сетями сигнализации (например, IP и ATM, ОКС7 и SIP/H.323 и т. п.);
- *ФО SIP-прокси-сервера (SIP Proxy Server Function, SPS-F)*:
  - *ФО маршрутизации (Routing Function, R-F)* — предоставляет информацию о маршрутизации вызова ФО MGC-F; может использовать протоколы ENUM и TRIP;
  - *ФО учёта стоимости (Accounting Function, A-F)* — собирает учётную информацию о вызовах для целей биллинга, а также обеспечивает аутентификацию, идентификацию и учёт в удалённых сетях; может использовать протоколы RADIUS и AuC.

Элементы уровня услуг и приложений:

- *ФО сервера приложений (Application Server Function, AS-F)* — обеспечивает выполнение услуг для одного или более приложений; использует протоколы SIP, MGCP, H. 248, LDAP, HTTP, CPL и XML;
- *ФО управления услугами (Service Control Function, SC-F)* — обеспечивает управление логикой услуг; использует протоколы INAP, CAP и MAR, открытые API типа JAIN и Parlay.

Физически элементы сети могут выполнять как одну, так и несколько функций, а также одна функция может быть распределена между несколькими элементами сети. Так, в модуле контроллера медиашлюзов могут быть реализованы MGC-F, CA-F, IW-F, R-F/A-F, SPS-F и др.

10.2.2. Протоколы в сетях Softswitch

10.2.2.1. Протокол MGCP

Протокол управления медиашлюзом (Media Gateway Control Protocol, MGCP) является внутренним протоколом для обмена информацией между функциональными блоками распределённого шлюза. Перенос сообщений протокола MGCP обеспечивает протокол UDP.

Для описания процесса обслуживания вызова с использованием протокола MGCP разработана модель организации соединения, в основу которой положены два компонента: *оконечная точка или устройство (Endpoints)* и *подключение (Connections)*.

Оконечная точка — это порт оборудования, являющегося источником или приёмником информации. Порт может быть физическим или виртуальным. Каждый порт определяется идентификатором, содержащим доменное имя шлюза и локальное имя в шлюзе.

Соединение — подключение порта к одному из двух концов соединения, которое создаётся между ним и другим портом. Соединение может связывать порты разных шлюзов через сеть с IP-маршрутизацией или порты внутри одного шлюза.

При установлении, поддержании и разрушении соединения устройство управления и шлюз обмениваются командами и ответами, которые представляют собой набор текстовых строк.

Команды состоят из следующих компонент: *кода команды, идентификатора транзакции, идентификатора порта, версии протокола*.

В протоколе MGCP определены следующие команды:

- CreateConnection (CRCX) — создать соединение;
- ModifyConnection (MDCX) — модифицировать соединение;
- DeledeConnection (DLCX) — завершить соединение;
- Notify (NTFY) — уведомить;
- NotificationRequest (RQNT) — запрос уведомления;
- EndpointConfiguration (EPCF) — конфигурация портов;
- AuditEndpoint (AUEP) — проверить порт;
- AuditConnection (AUCX) — проверить соединение;
- ReStartInPrgress (RSIP) — рестарт.

Ответы состоят из следующих компонент: *кода ответа, идентификатора транзакции, комментария, параметров* (обязательных и не обязательных).

Определены следующие *основные параметры*:

- CallId (C) — идентификатор сеанса связи;
- ConnectionId (I) — идентификатор подключения;
- Mode (M) — режим соединения;
- RequestedInfo (F) — запрашиваемая информация;
- ResponseAck (K) — подтверждение транзакции;
- BearerInformation (B) — закон кодирования;
- RequestIdentifier (X) — идентификатор запроса;

- LocalConnectionOptions (L) — параметры порта;
- RequestedEvents (R) — запрашиваемые события;
- SignalRequests (S) — требование передать сигнал;
- NotifiedEntity (N) — уведомляемый объект;
- DigitMap (D) — план нумерации;
- QuarantineHandling (Q) — карантинная обработка;
- DetectEvents (T) — выявляемые события;
- ConnectionParameters (P) — параметры соединения;
- RestartMethod (RM) — метод рестарта;
- ReasonCode (E) — код причины;
- RestartDelay (RD) — задержка рестарта;
- ObservedEvents (O) — обнаруженные события;
- LocalConnectionDescriptor (LCD) — локальные параметры соединения на передающей стороне;
- RemoteConnectionDescriptor (RCD) — удалённые параметры соединения на приёмной стороне.

10.2.2.2. Протокол Megaco/H.248

Для переноса сигнальных сообщений Megaco/H.248 могут использоваться протоколы UDP, TCP, SCTP или технология ATM.

Для описания процесса обслуживания вызова с использованием протокола Megaco разработана модель организации соединения, в основу которой положены два компонента: *порт (Termination)* и *контекст (Context)*.

Порты являются источниками и приёмниками речевой информации и могут быть физическими (аналоговые телефонные интерфейсы оборудования) или виртуальными (существующие только в течение разговорной сессии).

Контекст — это абстрактное представление соединения двух или более портов одного шлюза. Контекст имеет уникальный идентификатор.

При помощи протокола Megaco/H.248 контроллер может изменять свойства портов шлюза. Свойства портов группируются в дескрипторы, которые включаются в команды управления портами.

Megaco/H.248 определяет восемь команд, которые обеспечивают возможность управления и манипулирования контекстами и окончаниями:

- Add — добавить окончание к контексту;
- Modify — изменить свойства окончания;
- Subtract — удалить окончание из контекста;
- Move — переместить окончание из одного контекста в другой;
- AuditValue — определить текущее состояние окончания;
- AuditCapabilities — определить состояния, которые может принимать окончание;
- Notify — уведомить о событиях, которые произошли в транспортном шлюзе;
- ServiceChange —уведомить об изменении обслуживания.

Megaco/H.248 определяет ряд дескрипторов, предназначенных для использования вместе с командами и ответами:

- дескриптор модема — специфицирует тип модема и связанные с ним параметры, которые следует использовать в соединениях модема при передаче аудио, видео или данных;
- дескриптор мультиплексирования — характеризует тип мультиплексирования в мультимедийном терминале;
- дескриптор среды — описывает различные информационные потоки (медиапотоки);
- дескрипторы потока — используются между MG и Softswitch для указания, какие медиапотоки взаимосвязаны;
- дескриптор среды — описывает различные информационные потоки (медиапотоки);
- дескрипторы LocalDescriptor и RemoteDescriptor — содержат или не содержат несколько описаний сеансов SDR, определяющих сеанс на локальном и удалённом концах соединения соответственно;
- дескриптор событий — содержит RequestIdentifier и список событий, которые MG должен обнаруживать;
- дескриптор сигналов — содержит список сигналов, которые должно подавать оконечное оборудование;
- дескриптор проверки — задаёт перечень информации, которую необходимо передавать из MG в Softswitch;
- дескриптор ServiceChangeDescriptor — используется только в сочетании с командой ServiceChange и включает в себя тип изменения обслуживания, причину изменения обслуживания и новый адрес для использования после изменения обслуживания;
- дескриптор DigitMap — описывает план нумерации;
- дескриптор StatisticsDescriptor — содержит информацию, которая относится к использованию оконечного оборудования в данном контексте;
- дескриптор ObservedEvents — используется для информирования Softswitch об обнаруженных событиях;
- дескриптор Error — передаётся в ответе, когда не может быть выполнена команда.

Команды могут группироваться в *транзакции*, причём в одной транзакции могут быть команды, относящиеся к разным контекстам. После приёма транзакции получатель последовательно выполняет команды, вложенные в неё.

Несколько транзакций могут передаваться по сети в виде *сообщений*, снабжённых заголовком, идентифицирующим отправителя. *Идентификатором сообщения (Message Identifier, MID)* служит назначенное имя (например, адрес в домене, имя в домене, имя устройства) объекта, передающего сообщение. Транзакции в пределах сообщения обрабатываются в произвольном порядке. Сообщения Megaco/H.248 по сути являются только транспортным механизмом.

Протокол Megaco/H.248 определяет типовые наборы характеристик, сигналов и событий для Softswitch и шлюзов разных типов, чтобы обеспечить возможность их взаимодействия. Типовой набор характеризуется базовым описанием, свойствами, предусматриваемыми событиями, поддерживаемы-

ми сигналами, предоставляемыми статистическими данными, любыми процедурами, относящимися к надлежащей поддержке набора. Он содержит следующие разделы:

- *Package* — содержит общее описание набора, определяющее его имя, идентификатор, текстовое описание, версию и опциональные поля;
- *Properties* — определяет свойства (характеристики) набора и содержит имя каждого свойства, его идентификатор, текстовое описание, тип, возможные значения, специфицирующие свойство и характеристики;
- *Events* — определяет событие и содержит имя события, его идентификатор, текстовое описание, параметры дескриптора Events и параметры дескриптора ObservedEvents;
- *Signals* — определяет сигналы, имя и идентификатор каждого сигнала, его текстовое описание, тип, продолжительность, дополнительные параметры;
- *Statistics* — определяет статистические данные, содержит имя и идентификатор данных каждого вида, их текстовое описание, единицы измерения;
- *Procedures* определяют дополнительные аспекты использования набора.

10.2.2.3. Протокол SIP

Протокол инициирования сеансов (Session Initiation Protocol, SIP) разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF [38, 39] и используется для организации, модификации и завершения сеансов связи. Протокол SIP не принимает непосредственного участия в передаче голосовых, видео и других данных, а лишь отвечает за установление связи.

В основу протокола рабочая группа MMUSIC заложила следующие принципы:

- персональная мобильность пользователей — услуги связи предоставляются вне зависимости от местонахождения пользователя;
- масштабируемость сети;
- расширяемость протокола — возможно дополнение протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

Кроме того, протокол SIP поддерживает преобразование имён, переадресацию, маршрутизацию, идентификацию и аутентификацию пользователя при его перемещении из одного места в другое.

В сети на базе SIP определены следующие элементы:

- *клиент UAC (User Agent Client)* — инициирует SIP-запросы;
- *сервер UAS (User Agent Server)* — принимает запросы и передаёт обратно ответы:
  - *прокси-сервер (Proxy Server)* — обрабатывает запросы пользователя;
  - *сервер переадресации (Redirect Server)* — предназначен для определения текущего адреса вызываемого пользователя;

- *сервер регистрации местоположения (Registrars / Location Server)* — позволяют агентам регистрировать своё местоположение, реализуя тем самым услуги мобильности.

Все сообщения SIP делятся на запросы клиента серверу и ответы сервера клиенту. Сообщения SIP могут переноситься как протоколом TCP, так и протоколом UDP. Все сообщения SIP представляют собой последовательности текстовых строк, структура и синтаксис которых соответствуют протоколу HTTP:

- *стартовая строка* — представляет собой начальную строку любого SIP-сообщения и содержит в случае запроса *тип запроса, текущий адрес узла-адресата, номер версии протокола*, а в случае ответа — *номер версии протокола, тип ответа, короткую расшифровку ответа*;
- *заголовки сообщений* — содержат информацию, необходимую для обработки сообщения:
  - *общие заголовки*: Call-ID (идентификатор соединения), Contact (контакт), CSeq (порядковый номер запроса/ответа), Date (дата), Encryption (кодирование), From (источник запроса), To (адресат), Via (путь), Record-Route (запись маршрута);
  - *заголовки содержания* — переносят информацию о размере тела сообщения или об источнике запроса;
  - *заголовки с дополнительной информацией о запросе*: Accept (принимается), Accept-Encoding (кодирование принимается), Accept-Language (язык поддерживается), Authorization (авторизация), Hide (скрыть), Max-Forwards (максимальное количество переадресаций), Organization (организация), Priority (приоритет), Proxy-Authorization (авторизация проксисервера), Proxy-Require (требование прокси-сервера), Route (маршрут), Response-Key (ключ кодирования ответа), Subject (тема), User-Agent (агент пользователя);
  - *заголовки с дополнительной информацией об ответе*: Allow (разрешение), Proxy-Authenticate (подтверждение подлинности прокси-сервера), Retry-After (повторить через некоторое время), Server (сервер), Unsupported (не поддерживается), Warning (предупреждение), WWWAuthenticate (аутентификация WWW-сервера);
- *тело сообщения* — содержит запросы (команды) SIP:
  - *INVITE* — приглашает пользователя принять участие в сеансе связи, и обычно содержит описание сеанса связи, вид принимаемой информации и параметры, необходимые для приёма информации;
  - *ACK* — подтверждает приём ответа на команду INVITE, содержит описание сеанса связи, переданное вызывающим пользователем;
  - *CANCEL* — отменяет обработку ранее переданных запросов;
  - *BYE* — разрушает соединение;
  - *REGISTER* — сообщает текущее местоположение пользователя;
  - *OPTIONS* — содержит информацию о возможностях терминального оборудования вызываемого пользователя;
  - *INFO* — используется для переноса между шлюзами сигнальных сообщений в течение сеанса связи, для переноса сигналов DTMF, созданных

в ходе сеанса, для переноса информации об остатке на счете (билинговой информации), для переноса между участниками сеанса связи изображений и другой не потоковой информации;
- *SUBSCRIBE* — подписка на предоставление информации о состоянии определённого ресурса;
- *MESSAGE* — предназначен для реализации служб интерактивного обмена текстовыми сообщениями с использованием модели, аналогичной отправке SMS.

Для организации взаимодействия с существующими приложениями IP-сетей и обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций используются SIP URL, которые бывают четырёх типов: `имя@домен`, `имя@IP-адрес`, `имя@хост`, `№телефона@шлюз`. Первая часть адреса идентифицирует пользователя, зарегистрированного в домене или на рабочей станции, а вторая часть — устройство или домен.

10.2.3. Протокол SDP

Протокол описания сессий (Session Description Protocol, SDP) [40] содержит механизм описания характеристик сеанса — время проведения, требуемые ресурсы и т.д. В SDP предусмотрена возможность изменения параметров сеансов в оперативном режиме.

SDP содержит следующие данные:
- информацию о медиапотоках;
- адреса назначения медиапотоков;
- номера UDP портов для отправителя и получателя;
- типы потока;
- медиаформаты, которые могут использоваться во время сессии;
- время начала, завершения и повторов сессии;
- информацию об инициаторе широковещательной сессии.

Описание сессии SDP:
- поле *Версия протокола* содержит версию протокола SDP;
- поле *Владелец / создатель и идентификатор сессии* служит глобальным идентификатором версии описания сессии:
  - username — идентифицирует пользователя;
  - session id — уникальный идентификатор сессии;
  - version — номер версии данного объявления;
  - network type — тип сети (например, «IN» — Интернет);
  - address type — тип адреса (например, «IP4» или «IP6»);
  - address — глобальный уникальный адрес хоста, с которого была создана данная сессия;
- поле *Имя сессии* указывает имя сессии;
- поле *Информация о сессии* может использоваться для определения медиапотока;

- поле *URI описания сессии* указывает на дополнительную информацию о конференции (сессии);
- поле *e-mail адрес*;
- поле *Телефонный номер*;
- поле *Информация о соединении* содержит данные о соединении:
  - network type — тип сети (например, «IN» — Интернет);
  - address type — тип адреса (например, «IP4» или «IP6»);
  - connection address — адрес соединения;
- поле *Информация о ширине полосы пропускания* определяет желаемую ширину полосы пропускания, которая должна использоваться сессией и медиапотоком;
- поле *Время* определяет время начала и конца сессии;
- поле *Интервалы повторения сессий*;
- поле *Объявление временной зоны* определяет сдвиги времени по отношению к базовому времени повторов сессий;
- поле *Криптографический ключ*;
- поле *Атрибуты сессии* могут быть определены как атрибуты «уровня сессии», атрибуты «уровня медиа»;
- поля *Имя медиа* и *Адрес транспорта*:
  - media — содержит тип медиапотока;
  - port — транспортный порт, в который будет передаваться медиапоток;
  - transport — транспортный протокол;
  - fmt list — форматы медиа.

10.2.4. Услуги в сетях Softswitch

Архитектура Softswitch даёт возможность операторам и/или провайдерам услуг предоставлять услуги, реализованные в виде приложений как от производителя Softswitch, так и от сторонних производителей, а также самостоятельно разрабатывать свои собственные приложения. Это возможно благодаря основанным на открытых стандартах прикладным программным интерфейсам API:

- Parlay — платформа для разработки, интеграции и развёртывания приложений на базе технологии Java;
- JAIN (Java Advanced Intelligent Network) — сетевая топология на базе Java, позволяющая осуществлять интеграцию протоколов IP и IN, обеспечивающая переносимость услуг, конвергенцию сетей и защищённый доступ как к телефонным сетям, так и к сетям передачи данных;
- CORBA (Common Object Request Broker Architecture) — открытая, независимая от поставщиков архитектура и инфраструктура, которую используют прикладные вычислительные системы для обеспечения их совместной работы в компьютерных сетях;
- XML (Extensible Markup Language) — язык разметки, который рассматривается как стандартный способ обмена информацией в средах, не использующих общие платформы;

– CPL (Call Processing Language) — язык, который может быть использован для описания и управления услугами IP-телефонии;
– CGI (Common Gateway Interface) — стандарт интерфейса, используемого для связи внешней программы с веб-сервером;
– сервисные Java-приложения.

10.3. Концепция IMS

Концепция *IMS (IP Multimedia Subsystem)* была предложена 3GPP в начале 2003 г. Эта концепция определяет сетевую архитектуру, которая опирается на пакетную транспортную сеть и обеспечивает управление сеансами связи и доставку в рамках этих сеансов любых типов информации — речи, данных, видео, мультимедиа. Следует заметить, что в системах, отвечающих концепции IMS, услуги могут предоставляться разными сервис-провайдерами и доставляться до пользователей по различным (проводным и беспроводным) сетям доступа.

Концепция IMS была стандартизована в спецификациях 3GPP R.5. Позднее к разработке спецификаций и стандартов IMS присоединились другие организации: 3GPP2, занимающаяся разработками для сетей CDMA2000, ETSI, группа Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), работающая в области конвергенции фиксированных сетей. Альянс Open Mobile Alliance (OMA) определил приложения и услуги, работающие поверх IMS, а Internet Engineering Task Force (IETF) — протоколы сетевого уровня. ETSI, отраслевые группы Форума мультисервисной коммутации (Multiservice Switching Forum, MSF) и Альянса для продвижения решений для телекоммуникационной отрасли (Alliance for Telecommunications Industry Solutions, ATIS) одобрили IMS в качестве основы сетевой инфраструктуры следующего поколения.

10.3.1. Архитектура IMS

Архитектура IMS (рис. 10.3) [41] представляет собой набор функций, соединённых стандартными интерфейсами (табл. 10.3). Физически элементы сети могут выполнять как одну, так и несколько функций, а также одна функция может быть распределена между несколькими элементами сети.

Выделяют три уровня:
– *пользовательский уровень или уровень передачи данных (User Plane)* — отвечает за подключение абонентов к инфраструктуре IMS;
– *уровень управления (Control Plane)* — отвечает за все действия по управлению сеансами связи (регистрирует абонентские устройства и направляет сигнальные сообщения протокола SIP к соответствующим серверам приложений);
– *уровень приложений (Application Plane)* — обеспечивает обслуживание конечных пользователей.

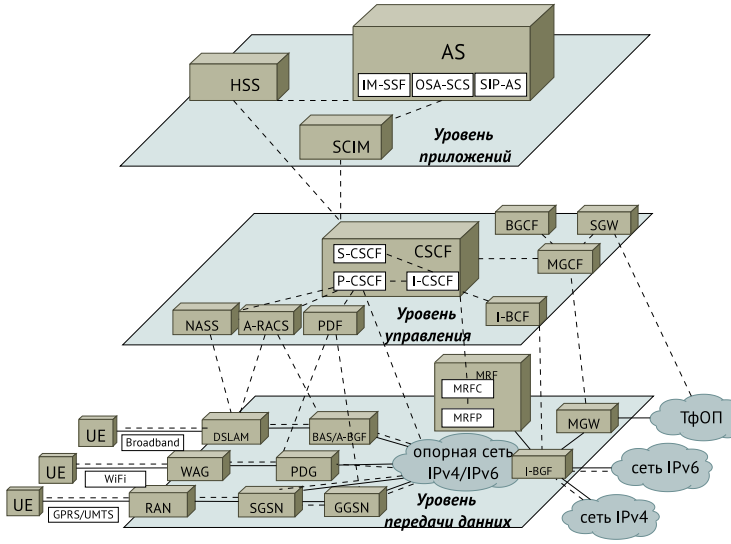

Рис. 10.3. Архитектура IMS (пунктирная линия — сигнализация, сплошная — данные)

Элементы уровня передачи данных:

- *функция обеспечения мультимедийных ресурсов (Media Resource Function, MRF)*:
  - *процессор мультимедийных ресурсов (MRF Processor, MRFP)* — обеспечивает обработку мультимедийных данных;
  - *контроллер мультимедийных ресурсов (MRF Controller, MRFC)* — обеспечивает реализацию услуг конференц-связи, оповещения или перекодирования передаваемого сигнала посредством управления MRFP при помощи протоколов сигнализации;
- *медиа-шлюз (Media Gateway, MGW)* — обеспечивает прямое и обратное преобразование потоков сетей с коммутацией пакетов в потоки сетей с коммутацией каналов;
- *функция межсетевого пограничного шлюза (Interconnect Border Gateway Function, I-BGF)* — обеспечивает взаимодействие между сетями IPv4 и IPv6, отвечает за обеспечение функций безопасности (трансляция адресов и портов NAPT, функции firewall, инструменты QoS);
- *шлюзовой узел GPRS (Gateway GPRS Support Node, GGSN)* — обеспечивает взаимодействие сети сотовой связи и инфраструктуры IMS;
- узел обслуживания абонентов GPRS (Serving GPRS Support Node, SGSN) — обеспечивает обработку данных абонентов GPRS;

- *сети радиодоступа (Radio Access Network, RAN)* — обеспечивают взаимодействие сотовых систем электросвязи и инфраструктуры IMS;
- *шлюз пакетной передачи данных (Packet Data Gateway, PDG)* — обеспечивает доступ пользовательского оборудования WLAN к инфраструктуре IMS, а именно ретранслирует IP-адреса, регистрирует пользовательское оборудование в IMS, обеспечивает выполнение функций безопасности;
- *шлюз беспроводного доступа (Wireless Access Gateway, WAG)* — обеспечивает соединение сетей WLAN и IMS;
- *функция пограничного шлюза доступа для широкополосного пользовательского оборудования (Access Border Gateway Function / Broadband Access Switch, A-BGF/BAS)* — обеспечивает доступ широкополосного пользовательского оборудования к инфраструктуре IMS;
- *цифровой абонентский шлюз доступа (Digital Subscriber Line Access Multiplexer, DSLAM)* — обеспечивает соединение абонентов, использующих широкополосный доступ к инфраструктуре IMS.

Элементы уровня управления:

- *функция управления вызовами и сеансами (Call Session Control Function, CSCF)* — обеспечивает доставку услуг реального времени посредством транспорта IP:
  - *обслуживающая CSCF (Serving CSCF, S-CSCF)* — обрабатывает все SIP-сообщения, которыми обмениваются оконечные устройства;
  - *прокси CSCF (Proxy CSCF, P-CSCF)* — обеспечивает обработку запросов от терминалов IMS к другим элементам IMS, а также выполняет ряд требований, относящихся к обеспечению безопасности (аутентификацию пользователя, контроль за корректностью передаваемых сигнальных сообщений, сбор данных о предоставленных пользователю сервисах);
  - *запрашивающая CSCF (Interrogating CSCF, I-CSCF)* — назначает S-CSCF для конкретного абонента, определяет привилегии абонента по доступу к услугам;
- *функция управления шлюзами (Breakout Gateway Control Function, BGCF)* — управляет маршрутизацией вызовов между сетью с коммутацией каналов (ТфОП или GSM) и сетью IMS;
- *функция управления медиа-шлюзами (Media GatewaysControl Function, MGCF)* — управляет соединениями в транспортных шлюзах IMS, используя H.248/ MEGACO;
- *шлюз сигнализации (Signaling Gateway, SGW)* — обеспечивает преобразование сигнализации ТфОП в вид, понятный MGCF;
- *подсистема управления ресурсами и доступом (Resource and Access Control, RACS)* — обеспечивает функции управления доступом в сеть, управление преобразованием сетевых адресов и портов, присвоение приоритета;
- *функция выбора политики (Policy Decision Function, PDF)* — определяет возможность организации сеанса или его запрета, необходимость изменения параметров сеанса и т.д.;

- *подсистема подключения сети (Network Attachment Subsystem, NASS)* — осуществляет динамическое назначение IP-адресов, аутентификацию на IPуровне, авторизацию доступа к сети, управление местонахождением на IPуровне.

Элементы уровня приложений:

- *элемент управления взаимодействием возможных услуг (Service Capability Interaction Manager, SCIM)* — обеспечивает управление взаимодействием плоскости приложений и ядра IMS;
- *SIP-сервер приложений (SIP Application Server, SIP AS)* — обеспечивает выполнение услуг на базе SIP;
- *сервер возможных услуг, базирующихся на открытом доступе к услугам (Open Service Access — Service Capability Server, OSA-SCS)* — обеспечивает доступ к услугам посредством стандартного программного интерфейса приложений;
- *сервер коммутации услуг (IP Multimedia – Service Switching Function, IM-SSF)* — служит для взаимодействия подсистемы IMS с услугами, разработанными для системы мобильной связи GSM;
- *сервер телефонных приложений (Telephony Application Server, TAS)* — принимает и обрабатывает сообщения протокола SIP, обеспечивает базовые сервисы обработки вызовов (включая анализ цифр, маршрутизацию, установление, ожидание и перенаправление вызовов, конференц-связь и т.д.), обеспечивает сервисную логику для обращения к медиасерверам при необходимости воспроизведения оповещений и сигналов прохождения вызова, отвечает за сигнализацию SIP к функции MGCF для выдачи команды медиашлюзам на преобразование битов речевого потока TDM (ТфОП) в поток IP RTP и направление его на IP-адрес соответствующего IP-телефона;
- *сервер домашних абонентов (Home Subscriber Server, HSS)* — обеспечивает открытый доступ в режиме чтения/записи к индивидуальным данным пользователя, связанным с услугами.

Таблица 10.3

Описание стандартных интерфейсов

Название интерфейса	Элементы IMS	Описание	Протокол
Cr	MRFC, AS	Используется MRFC для передачи данных (скриптов и др/ ресурсов) от AS	HTTP поверх TCP/SCTP
Cx	I-CSCF, S-CSCF, HSS	Используется для взаимодействия между I-CSCF/S-CSCF и HSS	Diameter
Dh	SIP AS, OSA, SCF, IM-SSF, HSS	Используется AS для поиска нужного HSS	Diameter
Dx	I-CSCF, S-CSCF, SLF	Используется I-CSCF/S-CSCF для поиска правильного HSS	Diameter

Таблица 10.3

Описание стандартных интерфейсов (продолжение)

Название интерфейса	Элементы IMS	Описание	Протокол
Gm	UE, P-CSCF	Используется для обмена сообщениями между UE и CSCF	SIP
Go	PDF, GGSN	Даёт возможность операторам управлять QoS на уровне передачи данных и обмениваться информацией между IMS и GPRS сетями	COPS (Rel5), Diameter (Rel6+)
Gq	P-CSCF, PDF	Используется для обмена политиками между P-CSCF и PDF	Diameter
ISC	S-CSCF, I-CSCF, AS	Используется для обмена сообщениями между CSCF и AS	SIP
Ma	I-CSCF -> AS	Используется для прямого перенаправления SIP-запросов, предназначенных серверам приложений (AS)	SIP
Mg	MGCF -> I-CSCF	MGCF преобразует сигнализацию ISUP в сигнализацию SIP и перенаправляет её в I-CSCF	SIP
Mi	S-CSCF -> BGCF	Используется для обмена сообщениями между S-CSCF и BGCF	SIP
Mj	BGCF -> MGCF	Используется для обмена сообщениями между BGCF и MGCF в некоторых сетях IMS	SIP
Mk	BGCF -> BGCF	Используется для прямого обмена сообщениями между BGCFs и IMS	SIP
Mm	I-CSCF, S-CSCF, IP-сеть	Используется для обмена сообщениями между IMS и IP-сетями	-
Mn	MGCF, IM-MGW	Даёт возможность управлять ресурсами уровня передачи данных	H.248
Mp	MRFC, MRFP	Используется для обмена сообщениями между MRFC и MRFP	H.248
Mr	S-CSCF, MRFC	Используется для обмена сообщениями между S-CSCF и MRFC	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	Используется для обмена сообщениями между несколькими CSCF	SIP
Rf	P-CSCF, I-CSCF, S-CSCF, BGCF, MRFC, MGCF, AS	Используется для offline-обмена информацией с CCF	Diameter
Ro	AS, MRFC	Используется для online-обмена информацией с ECF	Diameter
Sh	SIP AS, OSA SCS, HSS	Используется для обмена сообщениями между SIP AS/OSA SCS и HSS	Diameter
Si	IM-SSF, HSS	Используется для обмена сообщениями между IM-SSF и HSS	MAP

Таблица 10.3

Описание стандартных интерфейсов (продолжение)

Название интерфейса	Элементы IMS	Описание	Протокол
Sr	MRFC, AS	Используется MRFC для передачи документов (скриптов и др. ресурсов) для AS	HTTP
Ut	UE, AS (SIP AS, OSA SCS, IM-SSF)	Разрешает UE управлять информацией, касающейся его сервисов	HTTP(s)

10.3.2. Услуги в сетях IMS

Для реализации новых конвергентных услуг с гарантией качества обслуживания сервисная архитектура сети должна отвечать следующим требованиям:

- отделение уровней транспорта и доступа от сервисного уровня (прозрачность доступа);
- управление сеансом связи, в ходе которого задействуются несколько сервисов связи реального времени;
- совместимость с имеющимися сервисами интеллектуальной сети (IN), к которым относятся: определение имени вызывающей стороны, бесплатный номер (800), переносимость локального номера, сервисы, соответствующие стандартам CAMEL, ANSI-41 и т. д.;
- прозрачное взаимодействие с телефонными сетями (планы нумерации, сигнализация прохождения вызовов);
- конвергенция проводных и беспроводных сервисов;
- объединение голосовых услуг с сервисами реального времени (обмен мгновенными сообщениями);
- стандартизованные механизмы обмена пользовательской информацией между сервисами;
- стандартизованные механизмы аутентификации и биллинга конечных пользователей;
- стандартизованный, общий для всех сервисов графический пользовательский интерфейс;
- открытые стандартные интерфейсы и API для новых сервисов, разработанные сервис-провайдерами и третьими фирмами.

В сетях IMS определены следующие услуги:

- услуги, основанные на информации о присутствии и доступности пользователя — позволяют обеспечить доставку информации «правильному» человеку и/или на «правильное» устройство, т.е. при помощи протокола SIP можно обеспечить «прозрачное» переключение, например, между сотовой, WiFi или наземной связью с помощью одного устройства;
- услуги, основанные на информации о местоположении пользователя — позволяют предоставить пользователю информацию, актуальную для него

в данный момент (например, прогноз погоды, информация о дорожной ситуации и т.п.);
- единый механизм авторизации, не связанный с конкретным устройством или технологией;
- управление групповыми списками;
- групповое общение (Group Communication);
- Push-To-Talk — услуга, работающая в полудуплексном (half-duplex) режиме, когда сотовый телефон используется как терминал системы профессиональной мобильной радиосвязи (основное преимущество — возможность «группового вызова», т.е. общения по принципу «один–многие»);
- Push-To-Show;
- доска для записей (Whiteboard) — услуга, позволяющая двум или нескольким абонентам совместно редактировать рисунки и документы в режиме реального времени. Все, что делается одним участником сеанса, видят в режиме on-line все остальные участники;
- многопользовательские игры в реальном времени (шахматы и другие игры);
- голосовые вызовы с усовершенствованными функциями (Enriched Voice Calling) — включают видеотелефонию и возможность добавления к вызовам своего контента;
- совместное использование файлов в сети (File Sharing);
- обеспечение необходимого уровня безопасности.

10.3.3. Протокол SIP

Протокол SIP предназначен для управления сеансами связи (инициация, модификация, завершение). Использование SIP в IMS позволяет реализовать услугу конференц-связи, поскольку любое число абонентов может динамически подключаться к сеансу и выходить из него. Кроме того, SIP даёт возможность динамически в рамках существующего сеанса связи подключать новые услуги (например, сеанс связи можно начать с текстового чата, потом добавить голосовую связь, а затем при необходимости и видео). Наконец, средства SIP способны при инициации или модификации сеанса связи учитывать характеристики канала доступа и терминала каждого пользователя и задействовать их оптимальным образом.

10.3.4. Преимущества и недостатки IMS

IMS обладает следующими преимуществами:
- предоставление множества услуг — нет жёсткой привязки средств управления услугами и способа их доставки до абонента с самими услугами, внедрение принципиально нового сервиса не требует построения соответствующей инфраструктуры для его доставки;
- хорошая масштабируемость сети оператора — модернизировать инфраструктуру сети можно поэлементно (например, при увеличении объёма

трафика можно модернизировать только элементы уровня передачи данных, а при увеличении числа абонентов — элементы уровня управления);
- независимость IMS от специфики сетевого транспорта и каналов доступа делает её хорошей основой для конвергенции служб фиксированной и мобильной связи.

Недостатки IMS:
- для полноценного перехода к IMS операторам связи необходимо выстроить новую схему управления сеансами связи и модернизировать системы поддержки эксплуатации и бизнес-операций, а также обеспечить поддержку маршрутизаторами протокола IPv6;
- отсутствие терминалов, ориентированных на работу в IMSсетях, — оконечное оборудование должно уметь инициировать и обрабатывать IMSзапросы, поддерживать работу сложных приложений;
- отсутствие поддержки non-SIPприложений в рамках SIPориентированной архитектуры IMS.

10.4. Концепция A-IMS

В июле 2006 г. рабочая группа, в которую вошли ведущие поставщики телекоммуникационного оборудования Lucent Technologies, Cicso Systems, Motorola, Nortel и Qualcomm, под руководством оператора мобильной связи Verizon Wireless объявила о создании архитектуры *Advances to IMS (A-IMS)* [42–44].

Архитектура A-IMS [42, 44] является дальнейшим развитием стандарта IMS и призвана преодолеть его недостатки. Одной из проблем IMS является отсутствие поддержки non-SIPприложений в рамках имеющейся SIPориентированной архитектуры IMS. Архитектура A-IMS позволяет осуществлять взаимодействие между SIP и non-SIPприложениями, обеспечивает более полный policy-контроль над ними и управление сетевыми ресурсами, отвечающими за QoS, мобильность, безопасность, доступ и т.п. Включённые в архитектуру дополнения и усовершенствования применимы для построения сетей связи на основе разных технологий доступа (3G, xDSL, WiMax, Cable) или конвергентных VoIP-сетей.

Основные элементы A-IMS:
- *подсистема управления приложениями (Application Manager, AM)* — элемент управления SIPсессиями, выполняющий функции P-CSCF, I-CSCF, S-CSCF, BGCF;
- *подсистема управления данными об услугах (Services Data Manager, SDM)* — осуществляет хранение данных как для SIP, так и для non-SIPприложений, включает в себя функциональность HSS и AAA, а также (опционально) SLF (Subscriber Location Function), KMF (Key Management Function) и Accounting;
- *подсистема управления несущей (Bearer Manager, BM)* — осуществляет контроль на уровне транспортного потока (несущей): контролирует применение соответствующих политик, правил, осуществляет управление по-

токами данных PFO (Packet Flow Optimization), идентификацию вторжений;
- *подсистема управления безопасностью (Security Manager, SM)* — выполняет задачи мониторинга событий в сети, обнаружения аномалий на основе программных алгоритмов, управления элементами сети для отражения угроз, управления IDS/IDP и политиками безопасности;
- *подсистема управления политиками (Policy Manager, PM)* — обеспечивает общее управление и контроль над распределением ресурсов сети (QoS, PFO, mobility, access и т.п.); поддерживает как SIP, так и non-SIPприложения.

Дополнительные элементы A-IMS:
- *терминал доступа (Access Terminal, AT)* — оконечное устройство (фиксированное или мобильным), имеющее возможность предоставить доступ пользователей к услугам с помощью разных технологий (xDSL,WiFi, EVDO и т.п.);
- *шлюз IP (IP Gateway, IPGW)* — поддерживает взаимодействие между канальным и сетевым уровнями сети передачи данных, осуществляет аутентификацию устройств и переадресацию, отвечает за подсчёт пакетного трафика и обеспечение QoS;
- *посредник при предоставлении услуг (Service Broker, SB)* — представляет собой один из компонентов, отвечающих за механизм вызова (запуска) приложения с разных платформ (как использующих, так и не использующих SIP), при этом хранит логику предоставления услуг и управляет взаимодействием различных приложений на уровне сессий, являясь главным связующим звеном между SIP и non-SIPприложениями;
- *функция управления ключами (Key Management Function, KMF)* — хранит ключи (абонентские и сетевые), которые используются при аутентификации абонентских устройств;
- *Regulatory and PSTN Servers* — обеспечивают интерфейс для выполнения определённых задач перехвата вызовов и сбора информации для компетентных ведомств.

10.5. Определение и суть NGN

Сеть связи следующего поколения (ССП — Next Generation Network, NGN) — концепция построения сетей связи, обеспечивающих предоставление неограниченного набора услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счёт унификации сетевых решений, предполагающая реализацию универсальной транспортной сети с распределённой коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи.

В сети NGN предоставляют широкий выбор технологий доступа, поставщиков услуг и самих услуг. Кроме того, в сетях NGN пользователи получают доступ к услугам независимо от местоположения и технического окружения, что позволяет обеспечить единообразие в предоставлении услуг.

10.5.1. Основополагающие характеристики NGN

Архитектура NGN предполагает чёткое разделение между функциями обслуживания и функциями транспортировки, что позволяет предоставлять и развивать как существующие, так и новые услуги вне зависимости от используемой сети и типа доступа.

Сети NGN обладают следующими основными характеристиками:

- пакетная коммутация;
- разделение ресурсов между пропускной способностью канала-носителя, вызовом/сеансом, приложением/услугами;
- разделение между предоставлением услуг и транспортировкой, предоставление открытых интерфейсов;
- поддержка широкого спектра услуг, приложений и механизмов на основе унифицированных блоков обслуживания (включая услуги в режиме реального масштабе времени, в потоковом или автономном режиме, мультимедийные услуги);
- возможности широкополосной передачи со сквозной функцией QoS;
- взаимодействие с существующими сетями посредством открытых интерфейсов;
- универсальная мобильность;
- неограниченный доступ пользователей к разным поставщикам услуг;
- разнообразие схем идентификации;
- единые характеристики обслуживания для одной и той же услуги с точки зрения пользователя;
- сближение услуг между фиксированной и подвижной связью;
- независимость связанных с обслуживанием функций от используемых технологий транспортировки;
- поддержка различных технологий «последней мили»;
- выполнение всех регламентных требований, например, для аварийной связи, защиты информации, конфиденциальности, законного перехвата и т.д.

10.5.2. Преимущества сетей, базирующихся на концепциях NGN

Сети NGN имеют ряд преимуществ (как для пользователей, так и для операторов связи) по сравнению с другими сетями:

- для оператора:
  - построение одной универсальной сети для оказания различных услуг;
  - возможность оптимального использования полосы пропускания для интеграции различных видов трафика и оказания различных услуг;
  - больше возможностей по расширению сети и спектра услуг;
  - простота в управлении и эксплуатации;
  - возможность быстрого внедрения новых услуг и приложений с различным требованием к объёму передаваемой информации и качеству её передачи;

- для пользователя:
  - абстрагирование от технологий реализации услуг электросвязи;
  - гибкое получение необходимого набора, объёма и качества услуг;
  - мобильность получения услуг.

10.5.3. Спектр предоставляемых услуг

В сетях NGN могут предоставляться следующие услуги:

- услуги службы телефонной связи:
  - местное телефонное соединение,
  - междугороднее телефонное соединение,
  - международное телефонное соединение,
  - передача факсимильных сообщений между терминальным оборудованием пользователей,
  - организация модемных соединений между терминальным оборудованием пользователей,
  - переадресация вызова,
  - индикация вызова,
  - удержание вызова;
- услуги служб передачи данных:
  - выделенный канал передачи данных,
  - постоянный и коммутируемый доступа в сеть Интернет,
  - виртуальные частные сети передачи данных;
- услуги телематических служб:
  - электронная почта,
  - голосовая почта,
  - доступ к информационным ресурсам,
  - телефония по IP-протоколу,
  - аудиоконференция и видеоконференция;
- услуги служб подвижной электросвязи;
- услуги поставщиков информации:
  - видео и аудио по запросу,
  - интерактивные новости,
  - электронный супермаркет,
  - дистанционное обучение и др.

10.5.4. Архитектура NGN

С функциональной точки зрения сеть следующего поколения делят на две плоскости — *плоскость услуг (Service Stratum)* и *транспортную плоскость (Transport Stratum)* (рис. 10.4) [45, 46].

Плоскость услуг включает функции, отвечающие за передачу *услугоориентированных данных (Service-Related Data)*, и функции, отвечающие за управление и эксплуатационную поддержку ресурсов услуг и услуг сети, необходимых для предоставления пользователю услуг и приложений.

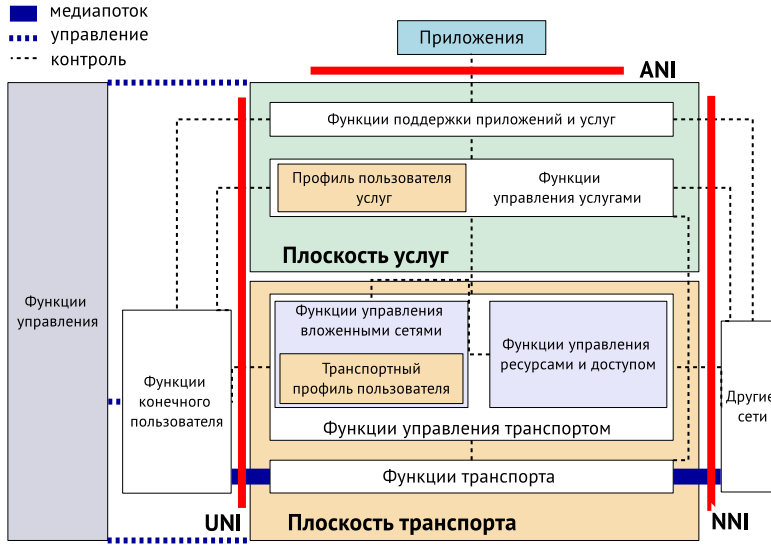

Рис. 10.4. Архитектура NGN

Транспортная плоскость включает функции, отвечающие за передачу данных, и функции, отвечающие за управление и эксплуатационную поддержку транспортных ресурсов для передачи этих данных между терминальными устройствами.

Взаимодействие приложений и элементов сети NGN осуществляется через *прикладной сетевой интерфейс (Application Network Interface, ANI)*.

Сетевой интерфейс пользователя (User Network Interface, UNI) обеспечивает взаимодействие функций конечного пользователя и элементов сети NGN.

Межсетевой интерфейс (Network Network Interface, NNI) обеспечивает взаимодействие сети NGN с другими сетями.

Так как сеть должна обеспечивать передачу разнородного трафика, в том числе чувствительного к задержкам, то немаловажными становятся такие требования к сети, как высокая надёжность оборудования узлов, поддержка функций управления трафиком, хорошая масштабируемость.

10.5.4.1. Функции транспортного уровня

Функции транспортного уровня обеспечивают соединение для всех компонентов и физически разделённых функций в рамках NGN, а также поддержку передачи медиаданных, контрольной и управляющей информации.

Определены следующие функции транспортного уровня:

- функции доступа к сети;
- функции граничного маршрутизатора;
- функции транзитного маршрутизатора;
- функции шлюза;
- функции обработки медианных;
- функции управления транспортным уровнем.

Функции доступа к сети (Access network functions) отвечают за доступ конечных пользователей в сеть, а также за сбор и оценку трафика, полученного транзитным узлом от пользователей. Кроме того, функции доступа к сети осуществляют управление качеством обслуживания, включая управление ёмкостью буфера, планирование и управление очередью, фильтрацию и классификацию трафика, его маркировку, применение политик по формированию трафика.

Функции доступа к сети классифицируются по технологиям доступа. Соответственно могут быть функции сетевого доступа по кабелю, оптоволокну, xDSL, по беспроводному соединению (IEEE 802.11 и 802.16 технологии, 3G RANдоступ).

Функции граничного маршрутизатора (Edge functions) используются для обработки данных и трафика в случае, когда трафик, приходящий из различных сетей доступа, сливается в один поток на границе домена NGN. Сюда входят функции, связанные с поддержкой QoS и контролем трафика.

Функции транзитного маршрутизатора (Core transport functions) отвечают за передвижение информации через сеть NGN и предоставляют средства для разделения трафика относительно требований к качеству обслуживания. Данные функции предоставляют QoSмеханизмы, непосредственно связанные с трафиком пользователя, включая управление буфером, размером очереди и планированием, фильтрацию пакетов, классификацию трафика, маркировку, разработку политик, контроль за точками доступа и возможностями брандмауэра.

Функции шлюза (Gateway functions) обеспечивают взаимодействие между функциями конечного пользователя и/или другими сетями, включая сети NGN, а также существующие сети, такие как, например, PSTN/ISDN, Интернет и т.д.

Функции обработки медианных (Media handling functions) предоставляют медиаресурсы, необходимые для предоставления услуг, таких как генерация тональных сигналов и преобразование одного кода в другой.

Функции управления транспортным уровнем (Transport control functions) включают в себя *функции контроля доступом к ресурсам (Resource and admission control functions, RACF)* и *функции контроля сетевых подключений (Network attachment control functions, NACFs)*.

Функции контроля доступа к ресурсам делают возможным представление для *функций управления услугами (Service Control Functions, SCF)* инфраструктуры транспортной сети в абстрактном виде и освобождают провайдеров от знания таких деталей, как топология сети, интерфейс подключения,

потребление ресурсов, механизмы QoS. Данные функции осуществляют контроль за ресурсами сети на основе заданной политики, обеспечивают резервирование ресурсов, взаимодействуют с функциями маршрутизатора с целью контроля за выполнением функций по фильтрации пакетов, классификации трафика, маркировке, определению политики, управлению приоритетами и т.д.

Функции контроля сетевых подключений осуществляют регистрацию пользователя на уровне доступа и инициализацию функций пользователя, необходимых для доступа к услугам NGN. Кроме того, они идентифицируют транспортный уровень, управляют адресным пространством сети, аутентифицируют сессию доступа.

Таким образом, функции контроля сетевых подключений обеспечивают:

- динамическое предоставление IP-адресов и других параметров конфигурации;
- определение возможностей оборудования пользователя и других параметров;
- аутентификацию пользователя и сети на IP-уровне, а также взаимную аутентификацию пользователя и сети;
- авторизацию доступа в сеть на основе профиля пользователя;
- конфигурацию доступа в сеть на основе профиля пользователя.

10.5.4.2. Функции уровня управления услугами

Абстрактное представление функциональных групп на уровне управления услугами состоит:

- из функций управления услугами, включая функции профиля пользователя услуги;
- из функций поддержки приложений и функций поддержки услуг.

Функции управления услугами (Service control functions) включают в себя функции управления ресурсами, регистрацией, аутентификацией и авторизацией на уровне услуг. Также могут включать в себя функции управления медиаресурсами, т.е. специализированными ресурсами и шлюзами сигнализации.

Функции управления услугами размещают профили пользователя, представляющие собой информацию о пользователя и другую управляющую информацию, в единый профиль пользователя на уровне услуг в форме базы данных. Эти базы данных могут быть определены и реализованы как набор сообщающихся баз данных с функциональными средствами, расположенными в любой части NGN.

Функции поддержки приложений и функций поддержки услуг (Application support functions and service support functions) включают в себя функции маршрутизации, регистрации, аутентификации, авторизации на уровне приложений. Эти функции доступны как функциональный группе приложений, так и функциональной группе пользователей. Функции поддержки приложений и функции поддержки услуг работают совместно с функциями управ-

ления услугами для обеспечения пользователей и приложений теми NGN-услугами, которые им требуются.

10.5.4.3. Функции конечного пользователя

Интерфейсы пользователей и сетевые интерфейсы, соединённые с сетью доступа NGN, могут быть любыми. Оборудование пользователя может быть как фиксированным, так и мобильным.

10.5.4.4. Функции управления

Поддержка управления фундаментальна для работы в NGN. Эти функции дают возможность управлять NGN с целью обеспечения NGN услуг ожидаемого качества, безопасности и надёжности.

Функции управления распределены по всем *функциональным модулям (Functional Entity, FE)* и взаимодействуют с сетевыми элементами управления и элементами управления услугами.

Функции управления применяются как на транспортном уровне, так и на уровне услуг NGN. Для каждого уровня они затрагивают следующие области:

- управление исходными настройками;
- управление конфигурациями;
- управление учётными записями пользователей;
- управление производительностью;
- управление безопасностью.

Функции управления учётными записями пользователей дают возможность провайдеру обеспечивать пользователей заказанными ими услугами.

10.5.5. Концепции NGN

10.5.5.1. Уровень мобильности в архитектуре NGN

Архитектура NGN поддерживает возможность обеспечения мобильности пользователей внутри и между различными сетями доступа и сетями с технологией мобильного доступа. Мобильность может быть поддержана на различных уровнях архитектуры NGN.

10.5.5.2. Архитектура услуг NGN

Архитектура услуг NGN состоит из трёх различных функциональных областей: области приложений, области функций поддержки приложений и функций поддержки услуг на сервисном уровне, области ресурсов транспортного уровня NGN.

Область функций приложений может быть разбита на две категории — всё, что связано с сетевыми провайдерами, и иное. К первой группе относятся сетевые провайдеры, субпровайдеры и т.д. Ко второй — независимые

провайдеры услуг, чей доступ к ресурсам должен быть аутентифицирован, контролируем и профильтрован функциями деблокиратора.

Посредством интерфейса ANI функциональная область функций поддержки приложений и услуг предлагает ресурсы услуг области приложений независимо от технологии сети. Также посредством ANI область приложений получает преимущества от использования возможностей и ресурсов функциональной области инфраструктуры NGN.

Архитектура услуг NGN следует трём основным функциональным характеристикам:

1. агностицизм — области функций поддержки приложений и функций поддержки услуг должны состоять из функций, независимых от инфраструктуры сети NGN;
2. поддержка официальных приложений и черт — архитектура услуг NGN не должна оказывать ограничивающее влияние на саму сеть NGN, т.е. должны поддерживаться функции по управлению сессиями, аутентификация, сведения о местонахождении и т.д.;
3. поддержка открытого интерфейса услуг — платформа услуг NGN должна предоставлять открытый интерфейс услуг (не зависящий от технологий транспортной сети), который обеспечивает доступ к таким функциям, как аутентификация, авторизация и безопасность, чтобы любой провайдер услуг мог воспользоваться возможностями сети.

10.5.5.3. Функции сокрытия сетевой топологии и просмотра трансляции сетевого адреса и порта

Сокрытие топологии уровня услуг достигается удалением или изменением топологической информации, передаваемой в прикладных сигнальных сообщениях одноранговой сети (например, в SIP-основанных приложениях топологическая информация находится в SIPзаголовках).

Сокрытие топологии транспортного уровня достигается путём изменения топологической информации в пакетах данных или посредством блокировки сетевых контрольных пакетов с топологической информацией (например, изменение IP-адресов и/или номеров портов в пакетах данных, пересекающих границу между сетью доступа и доменом).

Просмотр трансляции сетевого адреса и порта (Network Address and Port Translation, NAPT) осуществляет просмотр удалённого NAPT в сетях доступа.

10.5.5.4. Контроль за переполнением

Для защиты функциональных модулей управления сессиями от концентрации нежелательных запросов необходима реализация на границе сетей доступа следующих функций: обнаружение концентрации запросов путём сбора информации от двух или нескольких функциональных модулей, передача полученной информации о концентрации запросов другим функциональным модулям, управление трафиком в соответствии с информацией о концентрации запросов.

10.5.5.5. Функции управления учётными записями пользователей и тарификацией

Функции управления учётными записями пользователей и тарификацией предназначены для представления обобщённой архитектуры предоставления провайдерами услуг пользователям. Они описывают условия сбора и обработки информации о пользователях и заказанных ими услугах для предоставления её NGN-провайдеру. Данные функции включают в себя *функцию сбора данных для тарификации (Charging Trigger Function, CTF)*, *функцию тарификации online (Online Charging Function, OCF)*, *функцию хранения информации для тарификации (Charging Collection Function, CCF)*, *функцию определения стоимости (Rating Function, RF)*, *функцию управления учётными записями пользователей (Account Management Function, AMF)*.

Функция сбора данных для тарификации осуществляет сбор данных о полученных пользователями ресурсах и услугах сети. Кроме того, данная функция создаёт учётные (тарификационные) события, используя онлайновый учёт. Данные направляются онлайновой учётной функции (OCF) для получения авторизации для доступа к ресурсам сети на основе запроса пользователя.

Функция хранения информации для тарификации получает сведения о произошедших событиях от CTF. Затем эта информация используется для формирования тарификационных данных, передаваемых биллинговым доменам.

Функция тарификации online получает данные от CTF и обрабатывают их практически в режиме реального времени для предоставления авторизации использования сетевых ресурсов на основе запроса пользователя. OCF предоставляет квоту на использование ресурсов, которая должна отслеживаться CTF.

Функция определения стоимости определяет стоимость предоставляемого сетевого ресурса.

Функция управления учётной записью хранит баланс учётной записи пользователя во время работы онлайновой учётной функции. Баланс учётной записи пользователя должен определять объём оставшегося доступного трафика, время или содержание, а также количество денег на счёте.

10.5.6. Компоненты сети NGN

На уровне услуг определены два компонента — компонент услуг IPмультимедиа и компонент эмуляции сервиса PSTN/ISDN.

Компонент услуг IP-мультимедиа предоставляет посреднические услуги, включающие в себя управление услугами реального времени (голосовая или видео телефония, обмен сообщениями и т.п.), основанными на концепции IMS. В NGN IMS расширен для поддержки дополнительных видов сетей доступа, таких как xDSL и WLAN. Услуга имитации сетей PSTN/ISDN также обеспечивается этим компонентом.

Компонент эмуляции услуг PSTN/ISDN обеспечивает функционирование сетей на основе поддержки существующих услуг для интерфейсов пользователя и оборудования.

Эмуляция PSTN/ISDN относится к предоставлению услуг сетей PSTN/ISDN, используя адаптацию к IP-инфраструктуре. Компонент услуг эмуляции PSTN/ISDN делает возможным поддержку терминалов, связанных с IP-сетью, через шлюз. Все сервисы PSTN/ISDN остаются доступными и идентичными (т.е. с теми же операционными характеристиками), так что пользователи даже не подозревают, что они не соединены с TDM-основанным PSTN/ISDN.

На транспортном уровне также определены два компонента — *компонент функций контроля сетевых подключений (Network Attachment Control Functions, NACF)* и *компонент функций контроля доступом к ресурсам (Resource and Admission Control Functions, RACF)*.

Транспортные сети предоставляют соединения для всех компонентов и физически разделённых функций в рамках NGN. Транспортные сети подразделяются на сети доступа (Access Transport Networks) и внутренние сети (домены) (Core Transport Network) с шлюзом на границе, связывающим транспортные сети этих двух категорий. IP-соединение предоставляется оборудованию пользователя NGN на основе транспортных функций под контролем NACF- и RACFкомпонент.

NGN взаимодействует с другими сетями, например, с PSTN/ISDN и Internet. Причём взаимодействие происходит как на уровне услуг, так и на транспортном уровне, посредством граничных шлюзов.

10.5.7. Softswitch и IMS как концепции NGN

Softswitch и IMS реализуют концепцию NGN. Однако следует отметить их принципиально разные подходы к реализации принципов NGN.

Softswitch ориентируется на жёсткую структуру построения сети — регламентируются структура сети, интерфейсы, все компоненты сети (протоколы, кодеки и пр.). При организации сети на базе Softswitch подлежат выполнению все требования стандарта.

IMS демонстрирует модульную архитектуру, регламентируя интерфейсы, оставляя свободу выбора в компонентах (протоколах, кодеков и пр.). Сеть на базе IMS можно реализовывать постепенно, добавляя новые элементы, что позволяет удешевить внедрение.

Подход Softswitch представляется более стройным, в то время как подход IMS — более гибким, что и вызвало ориентацию последних стандартов NGN именно на IMS.

10.6. Универсальная система подвижной связи (UMTS)

Универсальная система подвижной связи (Universal Mobile Telecommunications System, UMTS) — сотовая телефонная система третьего поколения (3G).

Концепция UMTS — это своего рода философия создания универсальной основы, позволяющей поддерживать широкий спектр различных методов радиодоступа.

Основные характеристики:

- способ передачи данных — технология W-CDMA;
- скорость передачи информации — до 21 Мбит/с;
- широкий перечень услуг: видеозвонки, видеоконференции, высококачественные голосовые звонки, загрузка файлов с высокой скоростью, сетевые игры, мобильная комерция и др.

10.6.1. Структура UMTS

Основные уровни системы:

- наземная сеть радиодоступа стандарта UMTS (UMTS Terrestrial Radio Access Network, UTRAN) — совокупность сетевых элементов, обеспечивающих доступ абонентов к услугам сотовой связи;
- оборудование абонента (User Equipment, UE);
- ядро сети (Core Network, CN) — центральная система сети сотовой связи, отвечающая за установление соединений, аутентификацию абонентов, начисление платы за предоставленные услуги связи.

10.6.1.1. Элементы UTRAN

Контроллер сети радиодоступа системы UMTS (Radio Network Controller, RNC) 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.

RNC является эквивалентом контроллера базовой станции (BSC) сети GSM/GPRS, но выполняет гораздо больше функций нежели в системах сотовой связи второго поколения.

Базовая станция, или *Узел B*, системы сотовой связи стандарта UMTS (*NodeB*) преобразует сигнал, полученный от контроллера сети радиодоступа (RNC), в широкополосный радиосигнал, передаваемый к телефону.

Узел B является аналогом базовой станции (BTS) в сети GSM.

10.6.2. Оборудование абонента

Под *оборудованием абонента (UE)* понимается телефон, смартфон, ноутбук, стационарный компьютер и т.п. При помощи UE пользователь получает доступ к сети. UE является эквивалентом мобильной станции (MS) в GSM.

Оборудование абонента состоит из *оборудования подвижной связи (терминала)* и *универсального модуля идентификации обслуживания (USIM)*. Терминал уникально идентифицируется с помощью *IMEI*.

USIM обеспечивает персональную мобильность, предоставляя пользователю доступ к услугам, на которые абонент подписан. В отличие от SIM-карты в GSM карта USIM может поддерживать набор профилей. Каждый профиль может использоваться для регулирования доступных услуг в зависимости от возможностей терминала, в котором установлена карта USIM. И пользователь, и сеть могут регулировать профили.

10.6.2.1. Элементы подсистемы CN

В первых релизах стандарта UMTS (R99, R4) подсистема коммутации не отличалась по своей структуре от подсистемы коммутации сетей второго поколения. В неё входили:

- *центр коммутации (MSC)*, который выполнял функции коммутации, установления соединения, тарификации и др.;
- *регистры*, которые предназначены для хранения абонентских данных:
  - *домашний регистр местоположения (HLR)*;
  - *гостевой регистр местоположения (VLR)*;
  - *центр аутентификации (AUC)*.

В более поздних релизах (R5, R6, R7,R8) функции центра коммутации были разделены между двумя устройствами:

- *сервер центра коммутации (MSC-Server)* — отвечает за установление соединений, тарификацию, выполняет некоторые функции аутентификации;
- *шлюз среды центра коммутации (Media gateway, MGW)* — представляет собой коммутационное поле, подчинённое MSC-Server, обеспечивает передачу пользовательских данных.

В сети UMTS R5 HLR заменён на *сервер абонентов домашней сети (HSS)*, который включает в себя все функциональные возможности HLR и дополнительные функции для поддержки функций IM подсистемы IP-мультимедиа (IMS).

Подсистема IP-мультимедиа (IMS) является основным отличием сети UMTS R4 от R5, обеспечивает предоставление операторами мультимедийных услуг своим абонентам, базируясь на встроенных приложениях, услугах и протоколах Интернета.

Шлюз сигнализации (SGW) преобразует информацию сигнализации (в обоих направлениях) на транспортном уровне между сигнализацией на базе SS7 и сигнализацией на базе протоколов IP.

Функция шлюза сигнализации может быть реализована как отдельный элемент или внутри другого элемента.

Обслуживающий узел поддержки GPRS (Serving GPRS Support Node, SGSN) — аналог центра коммутации (MSC) для пакетной сети передачи данных GSM.

Функции SGSN:

- активация услуги передачи данных;
- обновление информации о местоположении абонентов при их перемещении между;
- инициация пейджинга абонентов при входящем запросе из внешних сетей передачи данных;
- начисление стоимости за оказанный объем услуг (биллинг).

Шлюзовой узел поддержки GPRS (Gateway GPRS Support Node, GGSN) — аналог G-MSC для пакетной сети в GSM, служит для передачи пакетных данных сетей сотовой связи стандартов GSM, UMTS, LTE во внешние сети, такие как Интернет.

GGSN конструктивно может быть выполнен в одном устройстве вместе с SGSN, а может быть реализован в виде отдельного устройства.

Глава 11. Сети 4G

11.1. WiMAX

11.1.1. Стек протоколов IEEE 802.16 (WiMAX)

WiMAX (Worldwide Interoperability for Microwave Access) — стандарт беспроводной связи IEEE 802.16 (рабочая группа создана в 1999 г.).

При зазработке ставились следующие задачи:

- обеспечение доступа к услугам информационных и коммуникационных технологий для небольших поселений, удалённых регионов, изолированных объектов;
- обеспечение доступа к услугам информационных и коммуникационных технологий более половины населения планеты.

Преимущества технологии:

- стандарт объединяет технологии как уровня оператора связи, так и технологии «последней мили»;
- беспроводные технологии более гибки и, как следствие, проще в развёртывании, так как по мере необходимости могут масштабироваться;
- простота установки как фактор уменьшения затрат на развёртывание сетей в развивающихся странах, малонаселенных или удалённых районах;
- на данный момент большинство беспроводных технологий широкополосной передачи данных требуют наличия прямой видимости между объектами сети; WiMAX благодаря использованию технологии OFDM создаёт зоны покрытия в условиях отсутствия прямой видимости от клиентского оборудования до базовой станции (диаметр соты порядка нескольких километров);
- изначально содержит протокол IP, что позволяет легко и прозрачно интегрировать её в локальные сети;
- подходит для фиксированных, перемещаемых и подвижных объектов сетей на единой инфраструктуре.

Характеристики:

- пропускная способность до 135 Мбит/с при полосе несущей 28 МГц;
- доступ к среде адаптивный, динамический;
- управление сетью централизованное.

11.1.1.1. Принципы работы WiMAX

Соединение между базовой станцией и клиентским приёмником производится в СВЧдиапазоне 2–11 ГГц. Такое соединение в идеальных условиях позволяет передавать данные со скоростью до 20 Мбит/с и не требует, чтобы станция находилась на расстоянии прямой видимости от пользователя. Этот режим работы базовой станции WiMAX близок широко распространённому

стандарту IEEE 802.11, что допускает совместимость уже выпущенных клиентских устройств и WiMAX.

Между соседними базовыми станциями устанавливается постоянное соединение с использованием сверхвысокой частоты 10–66 ГГц радиосвязи *прямой видимости*. Такое соединение в идеальных условиях позволяет передавать данные со скоростью до 120 Мбит/с.

Как минимум одна из базовых станций может быть постоянно связана с сетью провайдера через широкополосное скоростное соединение. Даже при небольшом количестве точек система способна корректно распределить нагрузку за счёт сотовой топологии.

На базе сотового принципа разрабатываются также пути построения оптимальной сети, огибающей крупные объекты, когда серия последовательных станций передаёт данные по эстафетному принципу. По структуре сети стандарта IEEE 802.16 очень похожи на традиционные сети мобильной связи: здесь тоже имеются базовые станции, которые действуют в радиусе до 50 км, при этом их также необязательно устанавливать на вышках. Для них вполне подходят крыши домов, требуется лишь соблюдение условия прямой видимости между станциями. Для соединения базовой станции с пользователем необходимо наличие абонентского оборудования. Далее сигнал может поступать по стандартному Ethernetкабелю как непосредственно на конкретный компьютер, так и на точку доступа стандарта IEEE 802.11 или в локальную проводную сеть стандарта Ethernet, что позволяет сохранить существующую инфраструктуру районных или офисных локальных сетей при переходе с кабельного доступа на WiMAX.

11.1.1.2. Режимы работы

Стандарт 802.16e-2005[1] вобрал в себя все ранее выходившие версии и на данный момент предоставляет следующие режимы:

- стационарный доступ (Fixed WiMAX) (рабочая группа IEEE 802.16d, стандарт IEEE 802.16-2004);
- сеансовый доступ (Nomadic[2] WiMAX);
- доступ в режиме перемещения (Portable WiMAX);
- мобильный доступ (Mobile WiMAX) (дополнение IEEE 802.16e-2005).

Fixed WiMAX. Фиксированный доступ представляет собой альтернативу широкополосным проводным технологиям (xDSL, T1). Стандарт использует диапазон частот 10–66 ГГц. Этот частотный диапазон из-за сильного затухания коротких волн требует прямой видимости между передатчиком и приёмником сигнала, но позволяет избежать одной из главных проблем радиосвязи — многолучевого распространения сигнала. При этом ширина каналов

[1] Документ IEEE 802.16e-2005 сам по себе является не стандартом, а дополнением к стандарту IEEE 802.16-2004.

[2] Буквально: кочующий.

связи в этом частотном диапазоне довольно велика (типичное значение — 25 или 28 МГц), что позволяет достигать скоростей передачи до 120 Мбит/с. Фиксированный режим включался в версию стандарта IEEE 802.16d-2004.

Nomadic WiMAX. Сеансовый доступ добавил понятие сессий к уже существующему Fixed WiMAX. Наличие сессий позволяет свободно перемещать клиентское оборудование между сессиями и восстанавливать соединение уже с помощью других вышек WiMAX, нежели те, что использовались во время предыдущей сессии. Такой режим разработан в основном для портативных устройств. Введение сессий позволяет также уменьшить расход энергии клиентского устройства.

Portable WiMAX. Для режима Portable WiMAX добавлена возможность автоматического переключения клиента от одной базовой станции WiMAX к другой без потери соединения. Однако для данного режима все ещё ограничена скорость передвижения клиентского оборудования — 40 км/ч.

Mobile WiMAX. Этот режим был разработан в стандарте 802.16e-2005 и позволил увеличить скорость перемещения клиентского оборудования до 120 км/ч. Основные достижения этого режима:

- устойчивость к многолучевому распространению сигнала и собственным помехам;
- масштабируемая пропускная способность канала;
- технология *Time Division Duplex (TDD)*, которая позволяет эффективно обрабатывать асимметричный трафик и упрощает управление сложными системами антенн за счёт эстафетной передачи сессии между каналами;
- технология *Hybrid-Automatic Repeat Request (H-ARQ)*, которая позволяет сохранять устойчивое соединение при резкой смене направления движения клиентского оборудования;
- распределение выделяемых частот и использование субканалов при высокой загрузке позволяет оптимизировать передачу данных с учётом силы сигнала клиентского оборудования;
- управление энергосбережением позволяет оптимизировать затраты энергии на поддержание связи портативных устройств в режиме ожидания или простоя;
- технология *Network-Optimized Hard Handoff (HHO)*, которая позволяет до 50 мс и менее сократить время на переключение клиента между каналами;
- технология *Multicast and Broadcast Service (MBS)*, которая объединяет функции DVB-H, MediaFLO и 3GPP E-UTRA для:
  - достижения высокой скорости передачи данных с использованием одночастотной сети;
  - гибкого распределения радиочастот;
  - низкого потребления энергии портативными устройствами;
  - быстрого переключения между каналами;

- технология *Smart Antenna*, поддерживающая субканалы и эстафетную передачу сессии между каналами, что позволяет использовать сложные системы антенн, включая формирование диаграммы направленности, пространственновременное маркирование, пространственное мультиплексирование;
- технология *Fractional Frequency Reuse*, которая позволяет контролировать наложение/пересечение каналов для повторного использования частот с минимальными потерями;
- размер фрейма в 5 мс обеспечивает компромисс между надёжностью передачи данных за счёт использования малых пакетов и накладными расходами посредством увеличения числа пакетов (и, как следствие, заголовков).

11.2. LTE

Сотовые сети стандарта GSM по своей структуре изначально не были предназначены для мобильного интернета. Соответственно, операторы сотовой связи вынуждены модернизировать сети до 3G (UMTS), и до 4G (LTE).

Сам термин LTE расшифровывается как Long Term Evolution и в переводе на русский означает «долгосрочная эволюция». Длительное время на роль связи 4G претендовал стандарт WiMAX, однако впоследствии был отодвинут на задний план как менее востребованный вариант быстрого беспроводного интернета.

LTE является следующим после 3G поколением мобильной связи и работает на базе IP-технологий. Основное отличие LTE от предшественников — высокая скорость передачи данных. Теоретически она составляет до 326,4 Мбит/с на прием (download) и 172,8 Мбит/с на передачу (upload) информации. При этом в международном стандарте указаны цифры в 173 и 58 Мбит/с, соответственно. Данный стандарт связи четвертого поколения разработало и утвердило Международное партнерское объединение 3GPP. Система кодирования — OFDM. Технология передачи —MIMO (Multiple Input Multiple Output).

Ортогональное частотное разделение каналов с мультиплексированием *(Orthogonal Frequency-division Multiplexing, OFDM)* — цифровая схема модуляции, использующая близко расположенные друг от друга ортогональные поднесущие в большом количестве. Все поднесущие моделируются по стандартной схеме модуляции, такой как квадратурная амплитудная модуляция на небольшой скорости символьной передачи с соблюдением общей скорости передачи данных, как и в простых схемах модуляции одной несущей в этой же самой полосе пропускания.

Данная технология описывает направление сигнала от базовой станции (БС) к мобильному телефону. Что же касается обратного пути сигнала, т.е. уже от телефонного аппарата к базовой станции, техническим разработчикам пришлось отказаться от системы OFDM и воспользоваться другой технологией под названием Single-carrier FDMA (SC-FDMA). В переводе SC-FDMA означает мультиплексирование на одной несущей. Смысл ее в том, что при

сложении большого количества ортогональных поднесущих образуется сигнал с большим пик-фактором (отношением амплитуды сигнала к своему среднеквадратичному значению). Для того чтобы такой сигнал мог передаваться без помех, необходим высококлассный и довольно дорогой высоколинейный передатчик.

MIMO *(Multiple Input Multiple Output)* представляет собой технологию передачи данных с помощью N-антенн и приема информации M-антеннами. При этом принимающие и передающие сигнал антенны разнесены между собой на такое расстояние, чтобы получить слабую степень корреляции между соседними антеннами.

11.2.1. Положение LTE в эфире

На данный момент под сети 4G уже зарезервированы диапазоны частот. Наиболее приоритетными принято считать частоты в районе 2,3 ГГц. Здесь главным примером является Китай со своим сотовым оператором China Mobile, уже выделившим нужный частотный диапазон и проводящий тестовое вещание. С учетом огромного объема местного потребления сотовой связи использование данной частоты обречено на успех и преобладание в Китае.

Другой перспективный диапазон частот — 2,5 ГГц применяется в США, Европе, Японии и Индии. Имеется еще частотная полоса в районе 2,1 ГГц, но она сравнительно небольшая – доступны лишь 15 МГц в диапазоне 2,1 ГГц, а большинство европейских мобильных операторов ограничивают в этом диапазоне полосы до 5 МГц. В будущем, скорее всего, наиболее используемым будет частотный диапазон 3,5 ГГц. Это связано с тем, что на данных частотах в большинстве стран уже используются сети беспроводного широкополосного доступа в интернет и благодаря переходу к LTE операторы получат возможность вновь применять свои частоты без необходимости приобретения новых дорогих лицензий. В случае необходимости под сети LTE могут быть выделены и другие диапазоны частот.

В отношении используемых полос частот и методов распределения в LTE все довольно непонятно и противоречиво, так как сам стандарт достаточно гибкий. В разных структурах сети четвертого поколения могут базироваться на полосах частот в диапазоне от 1,4 до 20 МГц, в отличие от фиксированных 5 МГц в 3G (UMTS). Также имеется возможность применения как временного разделения сигналов TDD *(Time Division Duplex — дуплексный канал с временным разделением)*, так и частотного — FDD *(Frequency Division Duplex — дуплексный канал с частотным разделением)*. Например, сеть LTE, строящаяся в Китае, является стандартом TD-LTE.

11.2.2. Сети LTE

Зона обслуживания базовой станции сети LTE может быть разной. Обычно она составляет около 5 км, но в ряде случаев она может быть увеличена до

30 и даже 100 км, в случае высокого расположения антенн (секторов) базовой станции.

Другое позитивное отличие LTE — большой выбор терминалов. Помимо сотовых телефонов, в сетях LTE будут использоваться многие другие устройства, такие как ноутбуки, планшетные компьютеры, игровые устройства и видеокамеры, снабженные встроенным модулем поддержки сетей LTE. А так как технология LTE обладает поддержкой хендовера и роуминга с сотовыми сетями предыдущих поколений, все данные устройства смогут работать и в сетях 2G/3G.

11.2.3. Структура сетей четвертого поколения

Сети LTE включают в себя модули сетей 2,75G (EDGE) и 3G (UMTS). Из-за данной особенности строительство сетей четвертого поколения будет достаточно специфичным и походит скорее на следующую ступень развития сегодняшних технологий, нежели на что-то принципиально новое.

К примеру, в соответствии с такой структурой звонок или интернет-сессия в зоне действия сети LTE может быть без разрыва соединения передана в сеть 3G (UMTS) или 2G (GSM). Кроме того, сети LTE довольно легко интегрируются с сетями WI-FI и Интернет.

По своей структуре сеть радиодоступа (Radio Access Network, RAN) — выглядит аналогично сети UTRAN UMTS, или eUTRAN, но имеет одно дополнение: приемо-передающие антенны базовых станций взаимосвязаны по определенному протоколу X2, который объединяет их в сотовую сеть — Mesh Network — и дает возможность базовым станциям обмениваться данными между собой напрямую, не задействуя для этого контроллер RNC — Radio Network Controller.

К тому же взаимосвязь базовых станций с системой управления мобильными устройствами (Mobility Management Entity, MME) и сервисными шлюзами (Serving Gateway, S-GW) осуществляется по принципу «многих со многими», что позволяет получить большую скорость связи с небольшими задержками.

11.2.4. LTE против WiMAX

В действительности стандарты LTE и WiMAX достаточно близки между собой. Они оба используют технологию кодирования OFDM и систему передачи данных MIMO. И в том, и в другом стандарте применяются FDD и TDD-дуплексирование при пропускной способности канала до 20 МГц. И обе системы связи используют в роли своего протокола IP. Соответственно, обе технологии в реальности одинаково хорошо применяют свой частотный диапазон и обеспечивают сравнимую скорость передачи данных интернет-доступа. Но, конечно, есть у них и некоторые отличия.

Одним из таких отличий является гораздо более простая инфраструктура сети WiMAX, а, следовательно, и более надёжная с технической точки зре-

ния. Данная простота стандарта обеспечивается его предназначением исключительно для передачи данных. С другой стороны, «сложности» LTE нужны для обеспечения ее совместимости со стандартами предыдущих поколений — GSM и 3G. И данная совместимость, безусловно, потребуется.

Существуют и другие детали в различии между LTE и WiMAX. Например, диспетчеризация радиочастотных ресурсов. В WiMAX она производится по технологии Frequency Diversity Scheduling, согласно которой поднесущие, предоставляемые абоненту, распределяются по всему спектру канала. Это необходимо для рандомизации и усреднения влияния частотно-селективных замираний на широкополосный канал.

В сетях LTE применена другая технология устранения частотно-селективных замираний. Она называется частотно-селективной диспетчеризацией ресурсов (Frequency Selective Scheduling). При этом для каждой абонентской станции и каждого частотного блока несущей создаются индикаторы качества канала CQI (Channel Quality Indicator).

Еще одним очень важным моментом, связанным с планированием сетей связи массового использования, является коэффициент переиспользования частот. Его роль — показывать эффективность использования доступной полосы радиочастот для каждой базовой станции в отдельности.

Базовая структура переиспользования частотного диапазона WiMAX состоит из 3-х частотных каналов. При использовании трехсекторной конфигурации сайтов (базовых станций определенного частотного диапазона), в каждом из секторов реализован один из 3-х частотных каналов. При этом коэффициент переиспользования частот равняется 3-м. Иными словами, в каждой из точек пространства имеется лишь треть радиочастотного диапазона.

Работа сотовой сети LTE (4G) производится с коэффициентом переиспользования частот равном 1. То есть, получается, что все базовые станции LTE работают на одной несущей. Внутрисистемные помехи в подобной системе сводятся к минимуму благодаря частотно-селективной диспетчеризации, гибкому частотному плану и координации помех между отдельными сотами. Абонентам в центре каждой соты могут даваться ресурсы из всей полосы свободного канала, а пользователям на краях сот предоставляются частоты только из определенных поддиапазонов.

Перечисленные выше особенности сетей LTE и WiMAX оказывают большое влияние на одну из их главных характеристик — степень радиопокрытия. Отталкиваясь от данного параметра, определяется необходимое количество базовых станций для качественного покрытия конкретной территории. Соответственно, он напрямую влияет и на конечную стоимость строительства сетей LTE.

Согласно расчётам, сеть LTE способна обеспечить лучшую зону покрытия при одинаковом числе базовых станций, что является несомненным плюсом для всех операторов сотовой связи.

11.2.5. Основные особенности LTE

LTE имеет следующие принципиальные особенности:

- Гибкое использование выделяемой полосы частот — возможно применение радиоинтерфейса LTE в полосе 1,5 МГц, 5 МГц, 10 МГц, 20 МГц. Чем шире используемая полоса частот, тем большими потенциальными возможностями располагает радиоинтерфейс.
- Использование для передачи информации технологии OFDM в совокупности с тремя возможными схемами информационного кодирования сигнала в зависимости от отношения сигнал/шум на входе приемника.
- Использование концепции ALL IP — передача всей информации с применением технологии коммутации пакетов. Построение наземного сегмента сети с интеграцией в существующей сети.
- Для хэндовера и роуминга используется концепция Mobile IP, что позволяет унифицировать обслуживание абонентских терминалов и интегрировать служебную информацию мобильной сети в общую служебную информацию.
- Для увеличения одновременно открытых сеансов связи с большим количеством оконечных и промежуточных устройств используется протокол IPv6.
- Использование большого количества «промежуточных» устройств — шлюзов, интеллектуальных маршрутизаторов, балансировщиков нагрузки, гейткипперов и т.д. для организации совместной работы большого количества абонентских устройств и приложений.
- Применение систем управления и мониторинга оборудования с возможностями изменения настроек в зависимости не только от потребности запускаемого приложения, но и от информации, поступающей с уровня управления бизнесом.

11.2.6. LTE-Advanced

Мобильная связь стандарта LTE-Advanced, одобренного МСЭ (Международным союзом электросвязи) осенью 2010 года, отвечает всем предъявляемым к связи четвертого поколения требованиям, чем не может похвастаться предварительная версия 3GPP LTE, которую относят к pre-4G.

Усовершенствование технологии мобильной связи позволило в сети повысить скорость (на принимающем устройстве пользователя до 300 Мбит/с), эффективность передачи данных, улучшить качество уже оказываемых услуг, интегрируясь при этом с существующими протоколами. Для сравнения, стандарт LTE, при возможной максимальной скорости в 100 Мбит/с, предоставляет только 20 Мбит/с, чтобы гарантировать высокоподвижным (поездам, автомобилям) и малоподвижным (пешеходам) абонентам равный доступ к сети.

При запуске беспроводной связи нового стандарта LTE-A не требуется менять оборудование, достаточно внести изменения в программное обеспече-

ние. Функция Carrier Aggregation (объединение (агрегации) несущих частот), которая используется в инновационном решении для технологии LTE-A, позволяет операторам комбинировать частотные диапазоны и далее использовать свободные для повышения скорости, управлять доступностью ресурса для конечного пользователя созависимо с его потребностями и нагрузкой на сеть.

Предметный указатель

Список иллюстраций

Список таблиц

Используемая литература

1. Hares S., Wittbrodt C. An Echo Function for CLNP (ISO 8473), RFC 1575. — 1994. — URL: http://www.faqs.org/rfcs/rfc1575.html.
2. Никольский Н. Н. Передача ОКС7 через IP // Сети и системы связи. — 2005. — № 7. — URL: http://www.ccc.ru/magazine/depot/05_07/0301.htm.
3. Самуйлов К. Е., Галентовская М. Введение в систему сигнализации № 7 // Сети. — 1999. — № 8-9. — URL: http://www.osp.ru/nets/1999/08-09/144246/_p1.html.
4. Bluetooth SIG, Inc. — URL: http://www.bluetooth.com/Bluetooth/.
5. IEEE 802.15 Working Group for WPAN. — URL: http://www.ieee802.org/15/.
6. Rosen E., Viswanathan A., Callon R. Multiprotocol Label Switching Architecture, RFC 3031. — 2001. — URL: http://www.ietf.org/rfc/rfc3031.txt.
7. MPLS Label Stack Encoding, RFC 3032 / E. Rosen, D. Tappan, G. Fedorkow et al. — 2001. — URL: http://www.ietf.org/rfc/rfc3032.txt.
8. LDP Specification, RFC 3036 / L. Andersson, P. Doolan, N. Feldman et al. — 2001. — URL: http://www.ietf.org/rfc/rfc3036.txt.
9. Stream Control Transmission Protocol, RFC 2960 / R. Stewart, Q. Xie, K. Morneault et al. — 2000. — URL: http://www.faqs.org/rfcs/rfc2960.html.
10. Ong L., Yoakum J. An Introduction to the Stream Control Transmission Protocol (SCTP), RFC 3286. — 2002. — URL: http://www.faqs.org/rfcs/rfc3286.html.
11. Mogul J., Deering S. Path MTU discovery, RFC 1191. — 1990. — URL: http://www.faqs.org/rfcs/rfc1191.html.
12. Floyd S., Handley M., Kohler E. Problem Statement for the Datagram Congestion Control Protocol (DCCP), RFC 4336. — 2006. — URL: http://tools.ietf.org/html/rfc4336.
13. Kohler E., Handley M., Floyd S. Datagram Congestion Control Protocol (DCCP), RFC 4340. — 2006. — URL: http://tools.ietf.org/html/rfc4340.
14. Ramakrishnan K., Floyd S., Black D. The Addition of Explicit Congestion Notification (ECN) to IP, RFC 3168. — 2001. — URL: http://tools.ietf.org/html/rfc3168.
15. ITU-T Recommendation Q.931: ISDN user-network interface layer 3 specification for basic call control. — 1998.
16. ITU-T Recommendation H.323 v1: Packet-based multimedia communications systems. — 1996.
17. ITU-T Recommendation H.245, Control protocol for multimedia communication. — 2006.

18. ITU-T Recommendation G.711 Pulse code modulation (PCM) of voice frequencies. — 1988.
19. ITU-T Recommendation G.723.1 Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s. — 1996, 2006.
20. Federal Standard 1016, Telecommunications: Analog to Digital Conversion of Radio Voice by 4,800 bit/second Code Excited Linear Prediction (CELP). — Washington : National Communications System, Office of Technology and Standards, 1991.
21. NCS Technical Information Bulletin 92-1. Details to Assist in Implementation of Federal Standard 1016 CELP.
22. ITU-T Recomendation G.728 Coding of speech at 16 kbit/s using law delay code excited linear prediction. — 1992.
23. ITU-T Recommendation G.729 Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction. — 1996.
24. ITU-T Recommendation G.729 — Annex A, Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACLEP), Annex A: Reduced complexity 8 kbit/s CS-ACELP speech codec. — 1996.
25. ITU-T Recommendation G.729 — Annex B. Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACLEP), Annex B: A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70. — 1996.
26. ITU-T Recommendation H.261: Video CODEC for audiovisual services at p X 64 kbit/s. — 1993.
27. Discrete-time signal processing. — 2nd edition Upper Saddle River edition. — NJ, USA : Prentice-Hall, Inc., 1999.
28. Алгоритмические основы растровой графики / Д. В. Иванов, А. С. Карпов, Е. П. Кузьмин и др. — Изд. ИНТУИТ, 2007. — 286 с.
29. ITU-T Recommendation H.263: Video coding for low bit rate communication. — 2005.
30. ITU-T Recommendation H.264: Advanced video coding for generic audiovisual services. — 2005.
31. ISO/IEC 14496-10 Standart «Information technology — Coding of audiovisual objects — Part 10: Advanced Video Coding». — 2005.
32. ITU-T Recommendation T.120: Transmission protocols for multimedia data. — 1996.
33. Иванцов И. Стеки протоколов // Журнал сетевых решений LAN. — 2007. — № 3.
34. ITU-T Recommendation H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communication systems. — 2006.
35. ITU-T Recommendation H.235.0, H.323 Security: Framework for security in H- series (H.323 and other H.245-based) multimedia systems. — 2005.
36. ITU-T Recommendation H.450.2: Call transfer supplementary service for H.323. — 1998.
37. ITU-T Recommendation H.450.3: Call diversion supplementary service for H.323. — 1998.

38. SIP: Session Initiation Protocol, RFC 2543 / M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg. — 1999.
39. SIP: Session Initiation Protocol, RFC 3261 / J. Rosenberg, H. Schulzrinne, G. Camarillo et al. — 2002.
40. Handley M., Jacobson V. SDP: Session Description Protocol, RFC 2327. — 1998.
41. Гулевич Д. С. Сети связи следующего поколения. — Открытые системы, ИНТУИТ, 2007. — URL: http://www.intuit.ru/department/network/ndnets/.
42. Duffy Jim. Verizon Wireless leads group offering IMS extensions // NetworkWorld.com. — 2006. — URL: http://www.networkworld.com/news/2006/072706-verizon-wireless-ims.html.
43. Duffy Jim. Verizon, others offer IMS extensions: Now comes the hard part for A-IMS // NetworkWorld.com. — 2006. — URL: http://www.networkworld.com/news/2006/073106-a-ims.html.
44. Хисматуллин Ильдар. IMS предлагается дополнить // Сети. — 2006. — № 14. — URL: http://www.osp.ru/nets/2006/14/3199456/.
45. ITU-T Recommendation Y.2011: General principles and general reference model for Next Generation Networks. — 2004. — URL: http://www.itu.int/rec/T-REC-Y.2011-200410-I/en.
46. ITU-T Recommendation Y.2012: Functional requirements and architecture of the NGN, release 1. — 2006. — URL: http://www.itu.int/rec/T-REC-Y.2012-200609-I/en.
47. Вишневский В. М., Портной С. Л., Шахнович И. В. Энциклопедия WiMAX. Путьк 4G. — М. : Техносфера, 2009. — 472 с.
48. Деев В. В. Методы модуляции и кодирования в современных системах связи. — СПб. : Наука, 2007. — 267 с.
49. WiMAX — технология беспроводной связи: основы теории, стандарты, применение / В. С. Сюваткин, В. И. Есипенко, И. П. Ковалев, В. Г. Сухоребров ; Под ред. В. В. Крылова. — СПб. : БВХ-Петербург, 2005. — 368 с.
50. Бакланов И. Г. NGN. Принципы построения и организации / Под ред. Ю. Н. Чернышова. — М. : Эко-Тренде, 2008. — 400 с.
51.
52. Воловодов А. От тактовой частоты до информационной магистрали // Сети и системы связи. — 1999. — № 9. — URL: http://www.ccc.ru/magazine/depot/99_09/read.html?0101.htm.
53. Беспроводные сети Wi-Fi / А. В. Пролетарский, И. В. Баскаков, Р. А. Федотов и др. — Изд-во «Интернет-университет информационных технологий — ИНТУИТ.ру», БИНОМ, 2007. — 216 с. — URL: http://www.intuit.ru/department/network/wifi/.
54. Лакнер Ханс. Мобильность и полоса пропускания. Обзор актуальных стандартов IEEE 802 за последний год // LAN. — 2007. — no. 6. — URL: http://www.osp.ru/lan/2007/06/4238886/.
55. Сети Fast Ethernet // Оптилинк. — 2001. — URL: http://www.optilink.ru/Techdoc/Ethernet/fast_ethernet.htm.

56. Смелянский Р. Л. Системы передачи данных и сети ЭВМ. — URL: http://www.kgtu.runnet.ru/WD/TUTOR/cn/index.html.
57. Основы локальных сетей. — 2005. — URL: http://www.intuit.ru/department/network/baslocnet/.
58. Кунегин С. В. Общее описание метода информационного обмена в сетях передачи данных Frame Relay. — 1998. — URL: http://kunegin.narod.ru/ref/fro/index.htm.
59. Филимонов А. Сети Frame Relay // Сети ЭВМ и телекоммуникации (курс лекций). — URL: http://lectures.net.ru/lectures/.
60. Мельников Д. Frame relay для профессионалов и не только // Сети. — 1997. — № 10. — URL: http://www.osp.ru/nets/1997/10/142934/.
61. Андронов С. О структуре и свойствах современных пакетных сетей // JetInfo. — 1999. — № 6(73). — URL: http://www.jetinfo.ru/1999/6/1/article1.6.1999.html.
62. Афонцев Эдуард. Metro Ethernet. Архитектура и технологии // NAG.ru. — 2005. — URL: http://www.nag.ru/2005/0227/0227.shtml.
63. Афонцев Эдуард. Назад в будущее. Metro Ethernet // NAG.ru. — 2005. — URL: http://www.nag.ru/2005/0212/0212.shtml.
64. Bluetooth в целом // Rainbow Technologies. — 2005. — URL: http://www.rtcs.ru/article_detail.asp?id=331.
65. Широков Ф. Bluetooth: на пути к миру без проводов // Открытые системы. — 2001. — № 2. — URL: http://www.radioscanner.ru/info/article95/.
66. Невдяев Леонид. Bluetooth — королевская технология // Сети. — 2000. — № 10. — URL: http://www.osp.ru/nets/2000/10/141423/.
67. Митилино Сергей. Беспроводные сети Bluetooth // Интернет и сети. — 2002. — URL: http://itc.ua/node/11177/.
68. Кессених В., Иванов Е., Кондрашов З. Bluetooth: принципы построения и функционирования // Chip NEWS. — 2001. — URL: http://www.chip-news.ru/archive/chipnews/200107/8.html.
69. Редькин Александр. Замена Bluetooth // Сети и Телекоммуникации. — 2005. — URL: http://www.citforum.ncstu.ru/nets/wireless/wireless_usb/.
70. Internet Protocol, RFC 791. — 1981. — URL: http://www.faqs.org/rfcs/rfc791.html.
71. Reynolds J., Postel J. Assigned numbers, RFC 990. — 1986. — URL: http://www.faqs.org/rfcs/rfc990.html.
72. Reynolds J., Postel J. Internet numbers, RFC 997. — 1987. — URL: http://www.faqs.org/rfcs/rfc997.html.
73. Braden R., Postel J. Requirements for Internet gateways, RFC 1009. — 1987. — URL: http://www.faqs.org/rfcs/rfc1009.html.
74. Hinden R. Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR), RFC 1517. — 1993. — URL: http://www.faqs.org/rfcs/rfc1517.html.
75. Rekhter Y., Li T. An Architecture for IP Address Allocation with CIDR,

RFC 1518. — 1993. — URL: http://www.faqs.org/rfcs/rfc1518.html.
76. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy, RFC 1519 / V. Fuller, T. Li, J. Yu, K. Varadhan. — 1993. — URL: http://www.faqs.org/rfcs/rfc1519.html.
77. Rekhter Y., Topolcic C. Exchanging Routing Information Across Provider Boundaries in the CIDR Environment, RFC 1520. — 1993. — URL: http://www.faqs.org/rfcs/rfc1520.html.
78. Deering S., Hinden R. Internet Protocol, Version 6 (IPv6) Specification, RFC 1883. — 1995. — URL: http://www.faqs.org/rfcs/rfc1883.html.
79. Deering S., Hinden R. Internet Protocol, Version 6 (IPv6) Specification, RFC 2460. — 1998. — URL: http://www.faqs.org/rfcs/rfc2460.html.
80. Краткий обзор протоколов информационно-вычислительных сетей. — 1999. — URL: http://cdo.bseu.by/library/ibs1/net_l/tcp_ip/net/frmp_ipv6.htm.
81. Hinden R., Deering S. Internet Protocol Version 6 (IPv6) Addressing Architecture, RFC 3513. — 2003. — URL: http://www.faqs.org/rfcs/rfc3513.html.
82. Blanchet M. A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block, RFC 3531. — 2003. — URL: http://www.faqs.org/rfcs/rfc3531.html.
83. Hinden R., Deering S., Nordmark E. IPv6 Global Unicast Address Format, RFC 3587. — 2003. — URL: http://www.faqs.org/rfcs/rfc3587.html.
84. OSI NSAPs and IPv6, RFC 1888 / J. Bound, B. Carpenter, D. Harrington et al. — 1996. — URL: http://www.faqs.org/rfcs/rfc1888.html.
85. Narten T., Draves R. Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 3041. — 2001. — URL: http://www.faqs.org/rfcs/rfc3041.html.
86. Postel J. Internet Control Message Protocol, RFC 792. — 1981. — URL: http://www.faqs.org/rfcs/rfc792.html.
87. Plummer David C. Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware, RFC 826. — 1982. — URL: http://www.faqs.org/rfcs/rfc826.html.
88. A Reverse Address Resolution Protocol, RFC 903 / Ross Finlayson, Timothy Mann, Jeffrey Mogul, Marvin Theimer. — 1984. — URL: http://www.faqs.org/rfcs/rfc903.html.
89. The Click Modular Router Project. — URL: http://www.read.cs.ucla.edu/click/.
90. Юшков Т. Архитектура MPLS. — 2005. — URL: http://www.mpls-exp.ru/mplsarchitecture.html.
91. Postel J. User Datagram Protocol, RFC 768. — 1980. — URL: http://www.faqs.org/rfcs/rfc768.html.

92. Postel Jon. Transmission Control Protocol, RFC 793. — 1981. — URL: http://www.faqs.org/rfcs/rfc793.html.
93. Mockapetris P. Domain names: Concepts and facilities, RFC 882. — 1983. — URL: http://www.faqs.org/rfcs/rfc882.html.
94. Mockapetris P. Domain names: Implementation specification, RFC 883. — 1983. — URL: http://www.faqs.org/rfcs/rfc883.html.
95. Mockapetris P. Domain names: Concepts and facilities, RFC 1034. — 1987. — URL: http://www.faqs.org/rfcs/rfc1034.html.
96. Mockapetris P. Domain names: Implementation specification, RFC 1035. — 1987. — URL: http://www.faqs.org/rfcs/rfc1035.html.
97. Ohta M. Incremental Zone Transfer in DNS, RFC 1995. — 1996. — URL: http://www.faqs.org/rfcs/rfc1995.html.
98. Vixie P. A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY), RFC 1996. — 1996. — URL: http://www.faqs.org/rfcs/rfc1996.html.
99. Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136 / P. Vixie, S. Thomson, Y. Rekhter, J. Bound. — 1997. — URL: http://www.faqs.org/rfcs/rfc2136.html.
100. Droms R. Dynamic Host Configuration Protocol, RFC 1541. — 1993. — URL: http://www.faqs.org/rfcs/rfc1541.html.
101. Faltstrom P. E.164 number and DNS, RFC 2916. — 2000. — URL: http://www.faqs.org/rfcs/rfc2916.html.
102. Захватов М. Качество обслуживания в операторских сетях. — URL: http://www.opennet.ru/docs/RUS/qos_oper/.
103. A Single Rate Three Color Marker, RFC 2697. — 1999. — September. — URL: http://www.ietf.org/rfc/rfc2697.txt.
104. A Two Rate Three Color Marker, RFC 2698. — 1999. — URL: http://www.ietf.org/rfc/rfc2698.txt.
105. A Time Sliding Window Three Color Marker (TSWTCM), RFC 2859. — 2000. — URL: http://www.ietf.org/rfc/rfc2859.txt.
106. Floyd S., Jacobson V. Random Early Detection gateways for Congestion Avoidance // IEEE/ACM Transactions on Networking. — 1993. — Vol. 1, no. 4. — P. 397–413. — URL: http://www.icir.org/floyd/papers/red/red.html.
107. Floyd Sally, Gummadi Ramakrishna, Shenker Scott. Adaptive RED: An Algorithm for Increasing the Robustness of RED's Active Queue Management. — 2001. — URL: http://www.icir.org/floyd/papers/adaptiveRed.pdf.
108. Low Latency Queueing. — 2001. — August. — URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt2/qcfconmg.htm.
109. Braden R., Clark D., Shenker S. Integrated Services in the Internet Architecture: an Overview, RFC 1633. — 1994. — URL: http://www.faqs.org/rfcs/rfc1633.html.
110. Resource ReSerVation Protocol (RSVP) — Version 1 Functional Specification, RFC 2205 / R. Braden, L. Zhang, S. Berson et al. — 1997. — URL:

http://www.faqs.org/rfcs/rfc2205.html.
111. Herzog S. RSVP Extensions for Policy Control, RFC 2750. — 2000. — URL: http://www.faqs.org/rfcs/rfc2750.html.
112. Wroclawski J. The Use of RSVP with IETF Integrated Services, RFC 2210. — 1997. — URL: http://www.faqs.org/rfcs/rfc2210.html.
113. Shenker S., Partridge C., Guerin R. Specification of Guaranteed Quality of Service, RFC 2212. — 1997. — URL: http://www.faqs.org/rfcs/rfc2212.html.
114. Wroclawski J. Specification of the Controlled-Load Network Element Service, RFC 2211. — 1997. — URL: http://www.faqs.org/rfcs/rfc2211.html.
115. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474 / K. Nichols, S. Blake, F. Baker, D. Black. — 1998. — December. — URL: http://tools.ietf.org/html/rfc2474.txt.
116. An Architecture for Differentiated Services, RFC 2475 / S. Blake, D. Black, M. Carlson et al. — 1998. — December. — URL: http://tools.ietf.org/html/rfc2475.txt.
117. Assured Forwarding PHB Group, RFC 2597 / J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. — 1999. — June. — URL: http://tools.ietf.org/html/rfc2597.
118. Jacobson V., Nichols K., Poduri K. An Expedited Forwarding PHB, RFC 2598. — 1999. — June. — URL: http://tools.ietf.org/html/rfc2598.
119. Grossman D. New Terminology and Clarifications for Diffserv, RFC 3260. — 2002. — April. — URL: http://tools.ietf.org/html/rfc3260.
120. Almquist P. Type of Service in the Internet Protocol Suite, RFC 1349. — 1992. — July. — URL: http://tools.ietf.org/html/rfc1349.
121. Brim S., Carpenter B., Faucheur F. Le. Per Hop Behavior Identification Codes, RFC 2836. — 2000. — May. — URL: http://tools.ietf.org/html/rfc2836.
122. Per Hop Behavior Identification Codes, RFC 3140 / D. Black, S. Brim, B. Carpenter, F. Le Faucheur. — 2001. — June. — URL: http://tools.ietf.org/html/rfc3140.
123. ITU-T Recommendation H.450.1, Generic functional protocol for the support of supplementary services in H.323. — 1998.
124. ITU-T Recommendation H.450.4: Call hold supplementary service for H.323. — 1999.
125. ITU-T Recommendation H.450.5: Call park and call pickup supplementary services for H.323. — 1999.
126. ITU-T Recommendation H.450.6: Call waiting supplementary service for H.323. — 1999.
127. ITU-T Recommendation H.450.7: Message waiting indication supplementary service for H.323. — 1999.
128. ITU-T Recommendation H.450.8: Name identification supplementary service for H.323. — 2000.
129. Вегешна Ш. Качество обслуживания в сетях IP. — 2003. — 368 с.

130. 3GPP TS 23.228. IP Multimedia Subsystem (IMS): Stage 2 (Release 8). — 2007.
131. 3GPP TS 23.517. Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture (Release 8). — 2007.
132. FCC, Part 68, Subpart F, Section 68.502. — URL: http://www.fcc.gov/Bureaus/Engineering_Technology/Documents/cfr/1999/47cfr68.pdf.
133. Таненбаум Эндрю. Компьютерные сети. — Четвёртое изд. — Питер : Питер, 2007. — С. 992.
134. Семёнов А. Ю. Протоколы Интернет. Энциклопедия 2-е изд. — 2005. — С. 1100.
135. Семёнов А. Ю. Алгоритмы телекоммуникационных сетей. — Изд-во Интернет-университет информационных технологий, Бином, 2007.
136. Гольдштейн А. Б., Гольдштейн Б. С. Softswitch. — БХВ — Санкт-Петербург, 2006.
137. Самуйлов К. Е. Методы анализа и расчёта сетей ОКС 7: Монография. — М. : Изд-во РУДН, 2002.
138. Халсалл Фред. Передача данных, сети компьютеров и взаимосвязь открытых систем. — М. : Радио и связь, 1995. — С. 408.
139. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для ВУЗов 3-е издание. — Питер : Питер, 2007. — С. 960.
140. Олифер В. Г., Олифер Н. А. Основы сетей передачи данных. Курс лекций. — Издательство: Интернет-университет информационных технологий, Бином, 2005. — С. 176.
141. Хогдал Дж. Скотт. Анализ и диагностика компьютерных сетей. — М. : Издательство «Лори», 2001. — С. 354.
142. Кульгин Максим. Практика построения компьютерных сетей. Для профессионалов. — СПб. : Питер, 2001. — С. 320.
143. Кульгин Максим. Технология корпоративных сетей. Энциклопедия. — СПб. : Питер, 2000. — С. 704.
144. Уолренд Джон. Телекоммуникационные и компьютерные сети. Вводный курс. — М. : Постмаркет, 2001. — С. 480.
145. Камер Дуглас Э. Компьютерные сети и Internet. Разработка приложений для Internet. — Третье изд. — М. : Издательский дом «Вильямс», 2002. — С. 640.
146. Снейдер Й. Эффективное программирование TCP/IP. Библиотека программиста. — СПб. : Питер, 2001. — С. 320.
147. Ефимушкин В.А., Ледовских Т.В. От E.164 к ENUM // Электросвязь. — 2002. — № 07. — С. 9–14.
148. Рекомендация МСЭ-Т E.164 Международной план нумерации электросвязи общего пользования. — 2005. — URL: http://www.itu.int/rec/T-REC-E.164-200502-I/ru.
149. RFC2916 E.164 Number and DNS. — URL: http://www.ietf.org/rfc/rfc2916.txt.
150. Федорушкин Илья. ENUM – нужна ли России альтернативная нумера-

ция? // Intelligent Enterprise. — 2006. — № 03. — URL: http://www.rtcomm.ru/about/press/pub/926.html.
151. Гринфилд Дэвид. За кулисами рынка IP-телефонии // LAN. — 2002. — № 04. — URL: http://www.osp.ru/lan/2002/04/136017/.

Содержание

Учебное издание

**К. Е. Самуйлов, Д. С. Кулябов, А. В. Королькова,
Ю. В. Гайдамака, И. А. Гудкова, П. О. Абаев**

Архитектура и принципы построения сетей связи следующих поколений

Учебное пособие

Технический редактор *Н. А. Ясько*
Дизайн обложки *М. В. Рогова*

Издание подготовлено в авторской редакции
Компьютерная вёрстка *А. В. Королькова*, *Д. С. Кулябов*

Подписано в печать ___.___.2013 г. Формат 60×84/16. Печать офсетная.
Усл. печ. л. ___. Тираж 100 экз. Заказ № ___.

Российский университет дружбы народов
115419, ГСП-1, г. Москва, ул. Орджоникидзе, д. 3

Типография РУДН
115419, ГСП-1, г. Москва, ул. Орджоникидзе, д. 3, тел. 952-04-41