Оглавление

Оглавление

Оглавление

Оглавление

Введение

Сеть связи (или телекоммуникационная сеть) — это технологическая система, которая состоит из каналов связи, узлов коммутации, оконечных станций и предназначена для обеспечения пользователей электрической связью с помощью абонентских терминалов, подключенных к оконечным станциям. Компьютерная сеть (инфокоммуникационная сеть) — это технологическая система, которая включает в себя, кроме сетей связи, также средства хранения, обработки и поиска информации и предназначена для обеспечения пользователей электрической связью и доступом к необходимой им информации.

Настоящий этап в развитии российских телекоммуникаций — это конвергенция сетей связи и компьютерных сетей.

Книга состоит из 26 глав, дополнений к трем главам и семи приложений.

В главе 1 рассматриваются общие положения Федерального закона «О связи» от 2003 года (редакция от 23.02.2011 года), Единой сети электросвязи России (ЕСЭ): роль и место ЕСЭ, классификация сетей. Приводится иерархический принцип построения ТфОП и GSM Российской Федерации, принцип коммутации каналов в этих сетях. Показана актуальность информационной безопасности сетей связи.

В главе 2 рассматривается принцип многоуровневого построения устройств сети связи. Приводится принцип коммутации пакетов, стек протоколов сети пакетной коммутации стандарта X.25, схема канального и сквозного шифрования информации в сети пакетной коммутации.

В главе 3 рассматриваются следующие основные функции физического уровня, относящиеся к сети X.25, а также некоторым другим технологиям сетей связи - архитектура физического уровня, физическая среда передачи сообщений, аналоговая и цифровая связь, модем, аналого-цифровое преобразование, цифровое кодирование, синхронизация, частотное и временное мультиплексирование, плезиохронная цифровая иерархия PDH.

В главе 4 приводится описание диаграммы последовательности обмена кадрами на канальном уровне сети X.25. Рассматриваются алгоритмы восстановления правильной последовательности при искажении в каналах связи. Приводятся три способа обнаружения ошибок с помощью циклического избыточного кода и приводятся примеры использования различных полиномов в сетях связи.

В главе 5 приводится описание структурных схем программного обеспечения (ПО) процедуры управления потоками по восстановлению информационных кадров второго

уровня сети X.25. Изложены основные положения составления ПО протоколов систем коммутации. В дополнении к главе приводятся алгоритмы программ, которые служат руководством по шести лабораторным работам студентов для освоения специфики разработки программного обеспечения узлов коммутации сетей связи.

В главе 6 приводится принцип установления виртуальных каналов в сети X.25. На примере сети X.25 с двумя центрами коммутации пакетов приводится описание диаграммы установления коммутируемого виртуального канала и передачи по нему пакета данных. Рассматривается замкнутая группа пользователей в качестве услуги, которая выполняет функцию информационной безопасности.

В главе 7 приводится описание структурных схем программного обеспечения следующих функций сетевого уровня X.25: распределение по типам принятых пакетов с канальных процессоров, формирование таблицы маршрутизации по логическим канальным номерам LCN, коммутация пакетов «данные». В дополнении к главе приводятся алгоритмы программ, которые служат руководством по двум лабораторным работам студентов для освоения специфики разработки программного обеспечения узлов коммутации сетей связи.

В главе 8 приводится стек протоколов сети Frame Relay (FR), выполнение требований пользователя по поддержке качества обслуживания, приводится диаграмма установления коммутируемого виртуального канала. Описывается схема построения виртуальных частных сетей на базе сети FR. Приводится возможность предоставления пользователям FR гарантий обслуживания сети с помощью соглашения SLA. Отмечены особенности сети FR по сравнению с сетью стандарта X.25.

В главе 9 приводятся основные положения и стек уровней сети пакетной коммутации ATM. Рассматриваются подуровни физического уровня ATM – конвергенция передачи и физическая передающая среда. Приводится пример размещения ячеек ATM в кадре цифровой иерархии PDH. Рассматривается сеть цифровой иерархии SDH: механизм устранения в ней недостатков PDH, типы оборудования, структура кадра на примере STM-1. Отмечается принцип размещения ячеек ATM в фиксированных позициях кадра.

В главе 10 рассматриваются функции, выполняемые на уровне ATM и уровне адаптации ATM. Приводится описание основных принципов функционирования протокола между ATM-коммутаторами по установлению коммутируемого виртуального канала по заданию пользователем требований на конкретные показатели качества обслуживания QoS и параметры трафика. Описывается схема построения виртуальных частных сетей на базе сети

ATM. Рассматриваются особенности сети ATM по сравнению с сетью Frame Relay.

В главе 11 рассматривается принцип работы первичных сетей уплотненного волнового мультиплексирования DWDM. Приводятся схемы типовых топологий участков системы DWDM – двухточечная, кольцевая, ячеистая.

В главе 12 приводится стек протоколов TCP/IP, включая протоколы информационной безопасности на прикладном, транспортном и межсетевом уровнях. Рассматривается пример переноса данных в IP-сети. Приводится краткое описание некоторых протоколов:

- прикладного уровня-простой протокол управления сетью SNMP;
- транспортного уровня - протокол управления передачей **TCP.**

В главе 13 изложены принципы маршрутизации в IP-сети, приводится краткое описание внутренних и внешних протоколов маршрутизации (RIP, OSPF, BGP). Рассматриваются протоколы обеспечения информационной безопасности ИБ в сети Интернет — на прикладном уровне (протокол PGP), на транспортном уровне (протокол SSL/TLS), на межсетевом уровне (протокол IPSec). Рассматривается использование протокола IPSec для создания с помощью туннельного режима виртуальной частной сети VPN (VPN-IPSec). Рассматриваются атаки DoS нарушения маршрутизации в IP-сети в результате передачи соседним маршрутизаторам нелегитимных сообщений обновления таблиц маршрутизации. Приводится описание защиты от этих атак.

В главе 14 рассматриваются две модели обеспечения качества обслуживания пользователей – интегральное и дифференцированное обслуживание. Приводится принцип алгоритма резервирования ресурсов с помощью протокола RSVP. На примере структурной схема программного обеспечения показана обработка очередей пакетов гарантированной пересылки. Рассматриваются стандарты ITU-T Y.1540 и Y.1541, касающиеся основных характеристик качества обслуживания QoS в IP-сетях.

В главе 15 рассматривается принцип работы сети MPLS, приводятся функциональные возможности стека меток. Рассматривается протокол распределения меток LDP. Приводится описание преимущества сети MPLS по сравнению с IP-сетью.

В главе 16 рассматриваются виртуальные частные сети MPLS третьего уровня. Описывается туннелирование в MPLS, на котором основано создание VPN MPLS.
Приводится описание принципов построения таблиц маршрутизации VPN третьего уровня с помощью протоколов IGP и MP-BGP. Приводится описание пересылки пакета данных между узлами VPN и формирование топологии VPN. Даётся сравнение VPN трёх топологий: на базе

сетей MPLS на третьем уровне, IP-сетей и ATM. Перечислены преимущества VPN на базе MPLS.

В главе 17 рассматривается функционирование цифровой сети с интеграцией служб ЦСИС (ISDN). Подробному описанию подлежит функционирование общеканальной сигнализации ОКС№7, входящей в ISDN - стек протоколов, диаграмма установления соединения в сети, функционирование подсистем передачи сообщений MTP на первом, втором и третьем уровнях, описание подсистемы пользователя ISUP. Приводится описание следующих алгоритмов обеспечения информационной безопасности в ISDN: Аутентификация пользователя в сети ISDN; аутентификация объектов аудиовизуальной службы сети ISDN и передача общих ключей симметричного шифрования сообщений.

В главе 18 рассматривается IP-телефония. Приводится описание состава и общих принципов работы сети по протоколу сигнализации SIP и по протоколу транспортировки данных по протоколу RTP. Приводятся угрозы ИБ и используемые механизмы защиты от них на базе протоколов TLS, S/MIME, HTTP Digest, AES и др.

В главе 19 рассматриваются функции подсистемы MTP по управлению сетью сигнализации ОКС№7: управление сигнальным трафиком, сигнальными звеньями и сигнальными маршрутами. Приводятся примеры: отказ и восстановление сигнального звена между исходящим и транзитными пунктами сигнализации; отказ и восстановление транзитного пункта сигнализации.

В главе 20 рассматривается принцип обслуживания вызовов в сети ТфОП/ISDN с предоставлением услуг с помощью интеллектуальной сети (IN). Приводится стек протоколов ОКС№7 в IN, даётся описание функций подсистемы управления соединением SCCP. Взаимодействие уровней стека протоколов показано на примере алгоритма предоставления реализованной на ЕСЭ России услуги PRM. Рассматривается алгоритм обеспечения информационной безопасности (аутентификация абонента - роумера) услуги «универсальная персональная связь» интеллектуальной сети.

В главе 21 приводятся способы множественного доступа пользователей, описание архитектуры системы GSM, принцип повторного использования частот. Дается описание использования логических каналов беспроводного доступа при установлении исходящего вызова от мобильной станции. Рассматривается обработка речевых сигналов на радиоучастке в устройствах АЦП, кодере речи, кодере канала, модуляторе. Приводятся примеры схем сверточного кода и перемежения. Приводятся алгоритмы информационной безопасности в GSM — конфиденциальность, аутентификация пользователя и приватность.

В главе 22 рассматривается архитектура протоколов передачи сигналов и использование ОКС№7 в GSM, а также иерархическая структура федеральной сети GSM. Приводится алгоритм установления вызова мобильной станции из ТфОП/ISDN. Дано описание некоторых атак «отказ в обслуживании» (DoS) маршрутизации ОКС№7 и их последствия в нарушении функционирования сетей связи общего пользования ТфОП/ISDN, IN, GSM России.

В главе 23 приводится краткое описание сетей стандартов GPRS и EDGE. Рассматривается принцип работы множественного доступа с кодовым разделением каналов CDMA и дается сравнение систем TDMA/FDMA и CDMA. Приводятся основные требования к сотовым сетям связи третьего поколения 3G, в основу которых положена система WCDMA. Приводится структура сети UMTS версии R99, а также краткие характеристики следующих версий. Рассматриваются ограничения в информационной безопасности сети GSM и алгоритмы решения этих проблем в сети UMTS - взаимная аутентификация пользователя и сети, установление алгоритмов обеспечения целостности сообщений и шифрования сообщений. В дополнении к главе для сети UMTS приводится описание угроз ИБ, требования по защите от них и количественная оценка угроз.

В главе 24 рассматривается архитектура сетей стандартов 802.11 в двух режимах – с точкой доступа и Ad Hoc. Приводится описание физического уровня и подуровня MAC сетей Wi-Fi (стандарты 802.11, 802.11a, 802.11b, 802.11g, 802.11n). Рассматривается архитектура mesh-сети на базе стандарта 802.11s. Приводится описание протоколов информационной безопасности сетей стандартов 802.11 – WEP, WPA, 802.11i для режима инфраструктуры (с точной доступа).

В главе 25 рассматриваются основные положения сетей WiMAX и LTE. Приводится описание частотного разделения каналов OFDM и режимов множественного доступа OFDMA и SOFDMA в сети WiMAX. Рассматриваются возможности WiMAX по предоставлению качества обслуживания QoS по требованиям пользователя. Приводится описание подуровня безопасности сети WiMAX. Приводятся основные требования к архитектуре сети LTE.

В главе 26 приводится краткое описание перспективных беспроводных самоорганизующихся сетей: мобильных целевых Ad Hoc сетей (MANET), беспроводных сенсорных сетей (WSN), ячеистых (Mesh) сетей (WMN) и автомобильных беспроводных сетей (VANET). При этом основное внимание уделяется информационной безопасности этих сетей в части анализа атак «отказ в обслуживании» (DoS) в результате намеренных действий

злоумышленника по нарушению работы протоколов маршрутизации.

Отметим отдельно вопросы обеспечения информационной безопасности (ИБ) современных технологий сетей связи, рассмотренные в указанных выше главах книги:

1. описание функционирования виртуальных частных сетей на базе сетей связи стандартов FR, ATM, TCP/IP, MPLS;
2. аутентификация пользователя сети ISDN, GSM, UMTS, стандартов IEEE 802.11, абонента-роумера одной из услуг сети IN;
3. аутентификация объектов аудиовизуальной службы и управление ключами в сети ISDN;
4. аутентификация сети UMTS абонентом этой сети, сети IN абонентом-роумером этой сети;
5. угрозы ИБ в IP-телефонии протоколу сигнализации **SIP;**
6. анализ угроз ИБ на радиоучастке сети UMTS;
7. защита приватных данных в GSM, UMTS;
8. угрозы нарушения маршрутизации в IP-сети и механизмы защиты от них;
9. угрозы нарушения маршрутизации в ОКС№7, примеры последствий этих атак «отказ в обслуживании» на функционирование сетей связи общего пользования ТфОП/ISDN, GSM, IN;
10. шифрование данных в GSM, UMTS, сети стандартов IEEE 802.11, сети WiMAX;
11. анализ угроз информационной безопасности в беспроводных самоорганизующихся сетях.

В книге приведены шесть приложений. В них изложены следующие вопросы обеспечения информационной безопасности, которые служат для использования при изучении основных глав. В приложении А изложены общие положения архитектуры сетевой безопасности в соответствии с рекомендацией международного союза электросвязи ITU-T X.805. Эта рекомендация закладывает основы разработки конкретных рекомендаций по этим вопросам для сетей связи с учетом их технологий. В приложении Б приводятся основные принципы шифрования с открытым ключом по алгоритму RSA, использование этого алгоритма в электронно-цифровой подписи и в создании общего секретного ключа взаимодействующих через сеть связи объектов. В приложении Г кратко изложены основные положения используемых в сетях связи алгоритмов аутентификации. В приложении Д приводятся основные принципы формирования общего секретного ключа с помощью метода

Диффи-Хеллмана. В приложении Е приводится дополнительно (к изложенному материалу в главе 13) описание алгоритма работы некоторых аспектов, связанных с повышением ИБ протокола прикладного уровня PGP. В приложении Ж приводится описание алгоритма работы протокола SET, который используется для защиты информации транзакций, проводимых через Internet, с помощью банковских операций. Протокол электронных платежных транзакций SET является стандартом, принятым основными платежными системами. Под транзакцией здесь понимается использование платежных средств для приобретения товара. Расчеты с использованием пластиковых карт – одна из форм электронных платежей через сеть связи.

В разделе «Контрольные вопросы» приводится список вопросов для проведения проверки знаний студентов на промежуточных этапах изучения дисциплины, в процессе проведения зачетов и экзаменов.

ГЛАВА 1. Единая сеть электросвязи России и актуальность информационной безопасности сетей связи

1.1. Роль и место ЕСЭ

С 1 января 2004 года вступил в силу новый Федеральный закон «О связи» [1], который определил начало нового этапа развития связи в России. Это этап развития российских телекоммуникаций – превращения российского общества на базе конвергентного объединения информатизации и телекоммуникации в электронно-цифровое общество. Сетевой основой российских телекоммуникаций определена Единая сеть электросвязи (ЕСЭ), в которую входят все сети электросвязи страны [2]. Отметим роль и место ЕСЭ.

ЕСЭ предназначена для удовлетворения потребностей населения, органов государственной власти и управления, обороны, безопасности, охраны порядка, а также хозяйствующих субъектов в услугах электросвязи. Устойчивая и качественная работа связи является важнейшим условием деятельности государства и общества.

ЕСЭ является одной из наиболее устойчивых секторов экономики России. В разные годы доля доходов за услуги связи в ВВП России страны составляла порядка 3-5 процентов.

ЕСЭ является катализатором для успешного развития других секторов экономики.

Для ЕСЭ России характерны следующие отличия по сравнению со многими развитыми странами мира:

- меньший уровень телефонизации и развития современных технологий;
- большое количество устаревшей аналоговой техники на сетях;
- большая территория России, значительные расстояния, большая неравномерность плотности населения, развития связи и Интернета по регионам России;
- ограниченность ресурсов радиочастотного спектра. В свое время в СССР основное внимание уделялось обороне и безопасности, что привело сегодня к необходимости решения сложных проблем конверсии спектра. В России освобождение спектра частот стоит дорого.
- различия в состоянии экономики и в уровне благосостояния населения.

Развитие ЕСЭ в соответствии с новым законом «О связи» должно проходить в следующем направлении:

1. дальнейшая либерализация рынка услуг электросвязи и расширение на нём справедливой конкуренции операторов связи;
2. дальнейшее развитие служб и спроса на них, особенно в части подвижной связи,

передачи данных, доступа в Интернет;

3. повышение требований к номенклатуре услуг электросвязи и к их качеству;
4. дальнейшее совершенствование телекоммуникационных и информационных технологий, их конвергенция;
5. усиление роли государственного регулирования в области связи в части взаимодействия сетей, осуществления надзора за деятельностью в области связи и др.

1.2. Классификация сетей связи

ЕСЭ Российской Федерации в соответствии со ст. 12 Федерального закона «О связи» состоит из следующих категорий:

- сеть связи общего пользования (**ССОП**);
- выделенные сети связи;
- технологические сети связи, присоединенные к сети связи общего пользования;
- сети связи специального назначения.

Сеть связи общего пользования предназначена для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации. ССОП Российской Федерации имеют присоединение к ССОП иностранных государств.

Примерами такой сети является телефонная сеть связи общего пользования ТфОП (**PSTN**, Public Switched Telephone Network). В России операторами междугородной и международной связи ТфОП являются ОАО «Ростелеком» и ОАО «МТТ» (Межрегиональный Транзит Телеком). «МТТ» стал с 2006 года первым альтернативным "Ростелекому" оператором дальней связи.

Сеть связи общего пользования, к которой может быть присоединено оборудование разных производителей, требует наличие стандартов. В следующем ниже списке указаны несколько организаций, занимающихся разработкой важных стандартов, и их местоположение в Интернете.

- Международный союз электросвязи, телекоммуникационный сектор стандартизации МСЭ-Т (**ITU-T**, International Telecommunications Union-Telecommunication Standardizing Sector). МСЭ-Т :финансируется Организацией Объединенных Наций.

- Европейский институт стандартов по телекоммуникациям (**ETSI**, European Telecommunications Standards Institute).
- Совет по архитектуре Интернета (**IAB**, Internet Architecture Board). Стандарты оформляются в виде технических отчётов **RFC** (Request for Comments) инженерной группой IETF (Internet Engeneering Task Force), входящей в IAB.
- Институт инженеров по электротехнике и электронике (**IEEE**, Institute of Electrical and Electronics Engineers). RFC издаются в целях стандартизации и развития протоколов Интернет.
- Международная организация по стандартизации (**ISO**, International Organization for Standardization).
- Альянс сотрудничества по сетям мобильной беспроводной сети третьего поколения 3GPP (3rd Generation Partnership Project).

Выделенные, технологические, а также сети связи специального назначения образуют группу сетей ограниченного пользователя (**ОгП**), так как контингент их пользователей ограничен корпоративными клиентами.

Выделенные сети связи – это сети, предназначенные для предоставления услуг ограниченному кругу ОАО "АСВТ" пользователей. Такие сети могут взаимодействовать между собой. Примерами операторов таких сетей являются ЗАО «Петерстар», ЗАО «РОСПАК» и др.

Технологические сети связи предназначены для обеспечения производственной деятельности организаций, управления технологическими процессами. Примерами операторов таких статей являются сети связи железнодорожного транспорта «Трансителеком ТТК», «ЕЭС Телеком», сеть «Газпром связь».

Сети связи специального назначения предназначены для обеспечения нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

По функциональному признаку разделяются на *сети доступа* и *транспортные сети*.

Транспортной является та часть сети связи, которая выполняет функции переноса (транспортирования) потоков сообщений от их источников из одной сети доступа к получателям сообщений другой сети доступа путём распределения этих потоков между сетями доступа.

Сетью доступа является та её часть, которая связывает источник (приёмник) сообщений с

узлом доступа, являющимся и транспортной сетью.

По типу присоединяемых абонентских терминалов сети ЕСЭ разделяются на:

- сети фиксированной связи, обеспечивающие присоединение стационарных абонентских терминалов;
- сети подвижной связи, обеспечивающие присоединение подвижных абонентских терминалов.

Примером сети доступа к транспортным сетям ТфОП и/или Интернет являются сети радиодоступа Wi-Fi, WiMAX и др.

По числу служб электросвязи сети бывают:

- *моносервисные*, предназначенные для организации одной службы электросвязи (например, телефония);
- *мультисервисные* (мультимедийные), предназначенные для организации нескольких служб (телефония, видео, передача данных).

Сети традиционно разделяются на первичные и вторичные.

Первичные сети представляют собой совокупность каналов и трактов передачи, образованных оборудованием узлов и линий передачи, соединяющих эти узлы. Первичные сети предоставляют каналы передачи во вторичные сети для образования каналов связи.

Вторичная сеть представляет собой совокупность каналов связи, образуемых на базе первичной сети путём их коммутации (маршрутизации) в узлах коммутации и организации связи между абонентскими устройствами пользователей.

Важной ролью в ЕСЭ Российской Федерации является развитие универсальной услуги. *Универсальные услуги связи* - услуги связи, оказание которых любому пользователю услугами связи на всей территории Российской Федерации в заданный срок, с установленным качеством и по доступной цене. В настоящий момент к универсальным услугам относятся:

- услуги телефонной связи с использованием таксофонов;
- услуги по передаче данных и предоставлению доступа к сети Интернет с использованием пунктов коллективного доступа.

При развитии инфокоммуникационных служб ЕСЭ предусматривается необходимость развития универсальной услуги в части расширения со временем её состава, а также координирование с её развитием в Европе.

1.3. Иерархический принцип построения ТфОП и GSM России

По территориальному делению ССОП России разделяются на несколько иерархический уровней. На рис. 1.1 приведена структура ТфОП России из четырёх уровней:

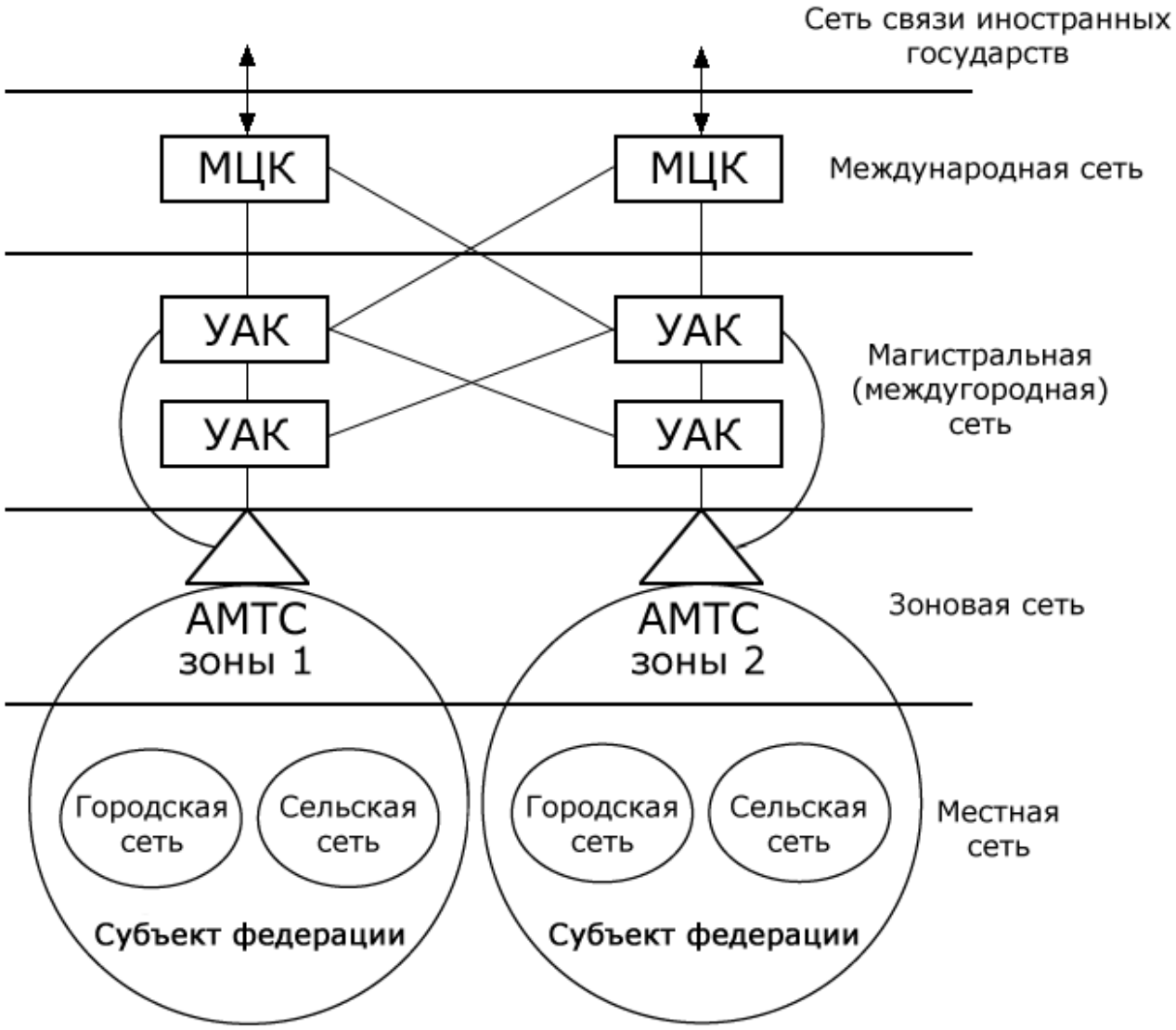


Рис. 1.1. Структура ТфОП Российской Федерации

1. местные сети, образуемые в пределах административной территории. Местные сети подразделяются на городские и сельские;
2. зоновые (региональные) сети, образуемые в пределах территории одного или нескольких субъектов Федерации (регионов). Всего в стране 89 зон;
3. магистральная (междугородная) сеть связывает между собой узлы субъектов Российской Федерации и узлы центра Российской Федерации. Магистральная сеть обеспечивает транзит потоков сообщений между зоновыми сетями с помощью узлов

автоматической коммутации (УАК), связанных между собой по схеме «каждый с каждым» (полносвязная схема). В ТфОП Российской Федерации действует восемь УАК, расположенных в городах Екатеринбург, Иркутск, Москва, Новосибирск, Ростов-на-Дону, Самара, Санкт-Петербург, Хабаровск. Шлюз между зоновыми сетями и магистральной сетью является автоматическая междугородная телефонная станция (АМТС). Каждая такая АМТС для надёжности связи соединена не менее, чем с двумя УАК, а также прямыми пучками каналов с АМТС других географических зон при соответствующем взаимном тяготении.

4. международная сеть общего пользования присоединена к сетям связи иностранных государств через международные центры коммутации (МЦК).

Крупные городские сети с ёмкостью до 8 млн номеров образуют ещё один иерархический уровень с узлами входящего и исходящего сообщений (**УИВС**). УИВС каждого района города соединён со всеми остальными узлами УИВС города. На такой сети размещается как минимум одна АМТС.

Такой принцип иерархического построения ТфОП позволяет избежать установления каналов связи между всеми узлами коммутации нижнего уровня, равного числу сочетаний по два числа этих узлов. Для ТфОП Российской Федерации отсутствие транзитного уровня магистральной сети при числе зоновых АМТС n=89 потребовало бы каналов связи между зоновыми АМТС. При использовании магистральной сети потребовалось 28 каналов между всеми восьми УАКами и 178 каналов между АМТС и УАКами.

Сети связи предоставляют одну службу (например, телефонию или передачу данных) или мультисервисные службы (телефон, видео, передача данных).

Федеральная сеть подвижной радиотелефонной связи общего пользования России стандарта GSM также построена по иерархическому принципу. Нижний уровень представляет сети отдельных операторов (одного или нескольких регионов страны) и верхний транзитный уровень, представляющий 7 транзитных центров коммутиации (ТЦК), соединённых по схеме «каждый с каждым». Место размещения ТЦК совпадает с расположением УАКов. Основное назначение транзитной сети – объединение сетей отдельных операторов в федеральную сеть GSM. В составе транзитной сети могут создаваться локальные центры коммутации (ЛЦК), размещённые в некоторых субъектах Федерации. ЛЦК представляют узлы доступа к транзитной сети от узлов субъекта Федерации, а также обеспечивают операторам подвижной и фиксированной связи межсетевое взаимодействие на местном уровне.

Сети связи по типам коммутации подразделяются на коммутацию каналов КК, коммутацию

пакетов КП (пакетную коммутацию ПК). Сети ТфОП или глобальная система связи с мобильными объектами GSM (Global System for Mobile communication) являются примерами сети КК.

При КК под соединение двух оконечных пользователей занимается физический канал, который не может использоваться для других соединений в сети в течение сеанса связи независимо от того, ведётся передача в данный момент или нет.

На рисунке 1.2. приведена диаграмма установления соединения и передачи информации в режиме коммутации каналов.

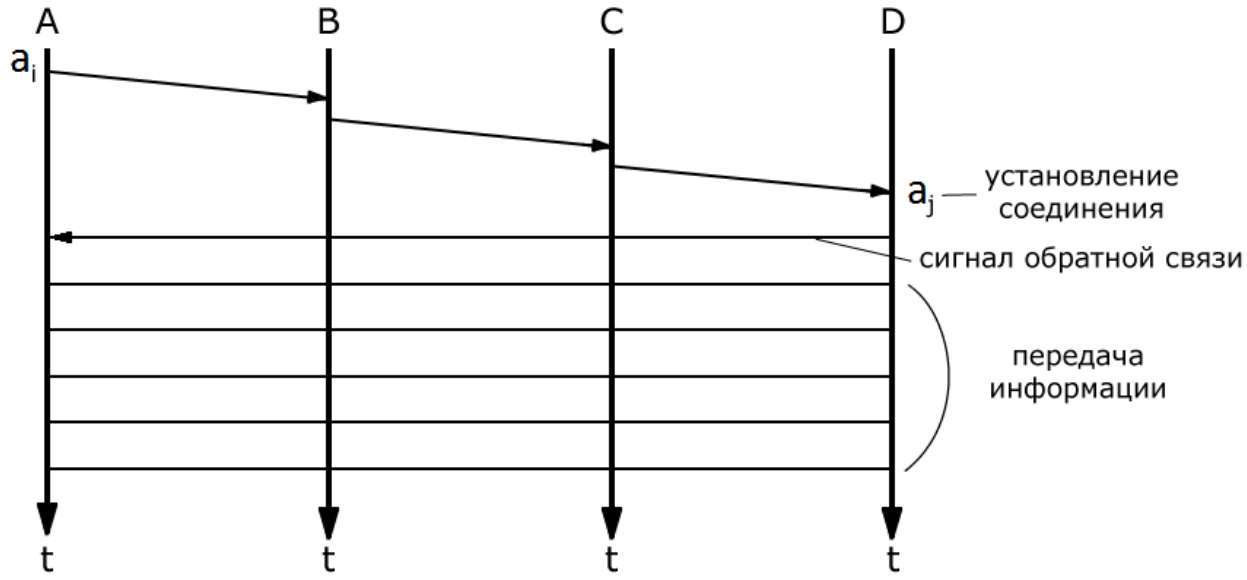


Рис. 1.2. Установление соединения и передача данных в сети КК

- Абонент a_i инициирует установление связи с абонентом a_j. Узел (коммутатор) связи A, используя адрес абонента a_j, выбирает физический канал с промежуточным узлом коммутации узлом B. Процедура повторяется с промежуточным узлом коммутации C и оконечным узлом коммутации D. После получения ответа с узла D устанавливается физическое соединение между абонентами a_i и a_j, а затем начинается передача данных.

Принцип коммутации пакетов приводится ниже при описании соответствующих технологий сетей связи.

1.4. Актуальность информационной безопасности сетей связи

При развитии ЕСЭ Российской Федерации большое внимание будет уделяться расширению номенклатуры услуг связи, повышению качества обслуживания, включая обеспечение информационной безопасности. Согласно ст. 7 закона «О связи» «операторы связи при эксплуатации сетей и сооружений связи обязаны обеспечить их защиту от НСД (несанкционированного доступа)». Под несанкционированным доступом согласно ГОСТ Р 52448-2005 [3] понимаются определённые критерии безопасности, в частности нарушения конфиденциальности, целостности и доступности информации и услуг. Большое внимание вопросам ИБ в сетях связи вызвано созданием в конце прошлого века нового принципа криптографии — асимметричной криптографии. Это позволило использовать сети связи для защищенного обмена между пользователями и для защищенного документооборота. Приведем некоторые примеры, показывающие актуальность обеспечения информационной безопасности в ЕСЭ России.

В плане реализации Федеральной Целевой Программы (ФЦП) «Электронная Россия» предусмотрены меры по повышению эффективности функционирования экономики, государственного управления и местного самоуправления. Многие проекты этой программы связаны с необходимостью реализации сетевой информационной безопасности [4-6].

Решение этих задач неразрывно связано с созданием в Российской Федерации межведомственной системы защищенного электронного документообмена (**ЭД**). Весьма существенной для такой системы является проблема обеспечения необходимого уровня информационной безопасности. Задача по созданию в Российской Федерации межведомственной системы защищенного ЭД является центральной в рамках создания и развития информационной телекоммуникационной системы специального назначения в интересах органов государственной власти РФ.

Важность защищенного ЭД отмечается в ФЦП «Электронная Россия» при совершенствовании взаимодействия органов государственной власти с органами местного самоуправления и хозяйствующими субъектами. При этом предусматривается:

- предоставление налоговой отчётности, таможенной документации;
- регистрация и ликвидация юридических лиц;
- получение лицензий и сертификатов;
- предоставление отчётной документации, предусмотренной законодательством об

акционерных обществах и о рынке ценных бумаг;

- получение охранных документов на объекты интеллектуальной собственности.

Комплекс мероприятий, позволяющих создать основу для успешного развития электронной торговли (ЭТ) в России является одним из главных направлений ФЦП «Электронная Россия». Первоочередным мероприятием является система ЭТ для государственных нужд. Внедрение ЭТ позволит уменьшить издержки государственных заказчиков при проведении конкурсов, сократить потери и злоупотребления. Реализация ЭТ для государственных нужд послужит катализатором широкомасштабного развития и использования этих методов в коммерческой деятельности. В первую очередь это касается малого бизнеса. Совершенствование платёжной системы является одним из ключевых элементов ЭТ. Важными требованиями к платёжной системе является защищённость сетей связи.

Другим направлением работ в соответствии с ФЦП «Электронная Россия» является создание системы мониторинга деятельности предприятий. Решением многих задач работы Счётной Палаты России является использование информационно-коммуникационных систем при контрольно-ревизионной деятельности. Обеспечение ИБ сетей связи является необходимым условием выполнения этих функций.

Информационная безопасность в сетях связи должна быть обеспечена также в таких направлениях ФЦП «Электронная Россия», как телемедицина (защита персональных данных), юридические и другие консультационные услуги (защита данных по расчетам).

Особое место занимает сетевая безопасность в электронной коммерции (ЭК) [7]. Под ЭК понимается разновидность коммерческой деятельности электронным способом с использованием сетей связи. Участниками этой деятельности являются покупатель, продавец, банк покупателя, банк продавца. Электронные расчёты, как вид безналичных расчётов, появились во второй половине XX века. Они приобрели принципиально новое качество, когда появились компьютерные сети связи. Качественный скачок выражается в том, что скорость осуществления платежей значительно возросла и появилась возможность их автоматической обработки. В электронной коммерции все документы создаются в цифровом виде и с помощью различных приложений обрабатываются и передаются в сеть связи.

Компьютерная сеть в качестве посредника между продавцом, покупателем и их банками доступна как для правомерных акций, так и для злоумышленников. Поэтому обеспечение ИБ в сетях связи при совершении финансовых транзакций является

необходимым условием реализации ЭК. Приведём описание некоторых областей ЭК, которые требуют обеспечения ИБ сетей связи. Системы ЭК, ориентированные на массового потребителя, стали широко использоваться с появлением сети Интернет. Классическим примером системы ЭК, когда все этапы коммерческой транзакции реализуются в электронном виде, является Интернет-магазин по продаже товаров. В банковской сфере активно используются системы обмена платёжными документами, в которых заключение сделка или договора производится в бумажном виде с применением обычных (рукописных) подписей, а реализация услуги, т.е. банковское обслуживание в электронном виде.

В последнее десятилетие в мире произошли революционные изменения в развитии мобильной связи. Это нашло отражение в широком охвате населения услугами сотовой телефонии, а также в развитии и внедрении новых технологий, среди которых выделяется технологии мобильной связи третьего и четвертого поколений. Как следствие этих процессов, уже несколько лет по всему миру продолжается бум мобильной коммерции (**m-commerce**), которая явилась новым логическим этапом развития электронной коммерции. Сегодня существенную часть рынка мобильной коммерции занимают платёжно-расчётные и финансовые услуги. Эти услуги можно разделить на несколько секторов:

1. банковские операции, включая оплату счетов, предоставление и погашение ссуд и кредитов;
2. платёжные операции с кредитными картами;
3. микроплатежи за услуги и товары.

На ранних стадиях развития рынка мобильных банковских и платёжных услуг владельцам мобильных устройств предлагались главным образом информационные услуги: проверка баланса счёта и совершённых транзакций. Сейчас получили широкое распространение услуги оплаты по счетам, денежные переводы и даже получение кредитов.

В настоящее время центр тяжести мобильных платежей смещается в область микроплатежей за мобильный контент, а также в область платежей торговым автоматам, за билеты, платежи в розничных торговых точках, такси и т.д. Все большую популярность приобретают мобильные платежи за парковку. В некоторых странах покупка билетов и оплата парковки через мобильную связь стали наиболее предпочтительным способом проведения таких операция для потребителей. Благодаря этому компании по управлению общественным транспортом и парковками существенно улучшили свои показатели, значительно сократив расходы на сбор и контроль платежей.

ГЛАВА 2. Стек протоколов сети пакетной коммутации X.25. Шифрование информации в сети

2.1. Многоуровневый принцип построения сети

Организация взаимодействия между устройствами в сети является сложной задачей. Как известно, для решения сложных задач используется универсальный прием – *декомпозиция*, то есть разбиение одной сложной задачи на несколько более простых задач-модулей. Процедура декомпозиции включает в себя четкое определение функций каждого модуля, решающего отдельную задачу, а также определение функций интерфейсов, связывающих каждый модуль. В результате достигается логическое упрощение задачи, а, кроме того, появляется возможность безошибочной модификации отдельных модулей без изменения остальной части системы, замена модулей.

При декомпозиции в сетях связи используют многоуровневый подход. Он заключается в следующем:

- все множество функциональных модулей разбивают на уровни;
- уровни организуют в виде вертикального стека, то есть они взаимодействуют на основе строгой иерархии;
- множество модулей, составляющих каждый уровень, формируется таким образом, что для выполнения своих задач они обращаются с запросами только к модулям, непосредственно примыкающего уровня, лежащего ниже в иерархии;
- с другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям соседнего уровня, лежащего выше в данной иерархии.

Такая иерархическая декомпозиция задачи предполагает четкое определение функций каждого уровня и интерфейсов между ними. Интерфейс определяет набор функций, которые уровень, лежащий ниже в иерархии, предоставляет уровню, лежащему выше. В результате иерархической декомпозиции достигается относительная независимость уровней, а значит, и возможность их легкой замены.

Количество уровней, их названия, содержание и назначение функциональных модулей разнятся от сети к сети. Однако во всех сетях целью каждого уровня является предоставление неких служб для верхних уровней, скрывая от них детали реализации предоставляемого сервиса.

Уровень **n** узла сети (одной машины), поддерживает связь с уровнем **n** другого узла сети. Правила и соглашения, используемые в данном общении, называются **протоколом** уровня **n.** По сути, протокол является договоренностью общающихся сторон о том, как должно происходить общение.

Протокол — это набор формализованных правил, процедур, спецификаций, определенный формат и способ передачи данных.

Обычно протокол обеспечивает взаимодействие между процессами, находящимися на одном иерархическом уровне, но в разных оконечных и транзитных пунктах сети. Элементы данных, пересылаемых на одном иерархическом уровне, называются элементами данных протокола блока данных PDU (Protocol Data Unit).

На рис. 2.1. показана пятиуровневая сеть. Объекты различных узлов сети включают

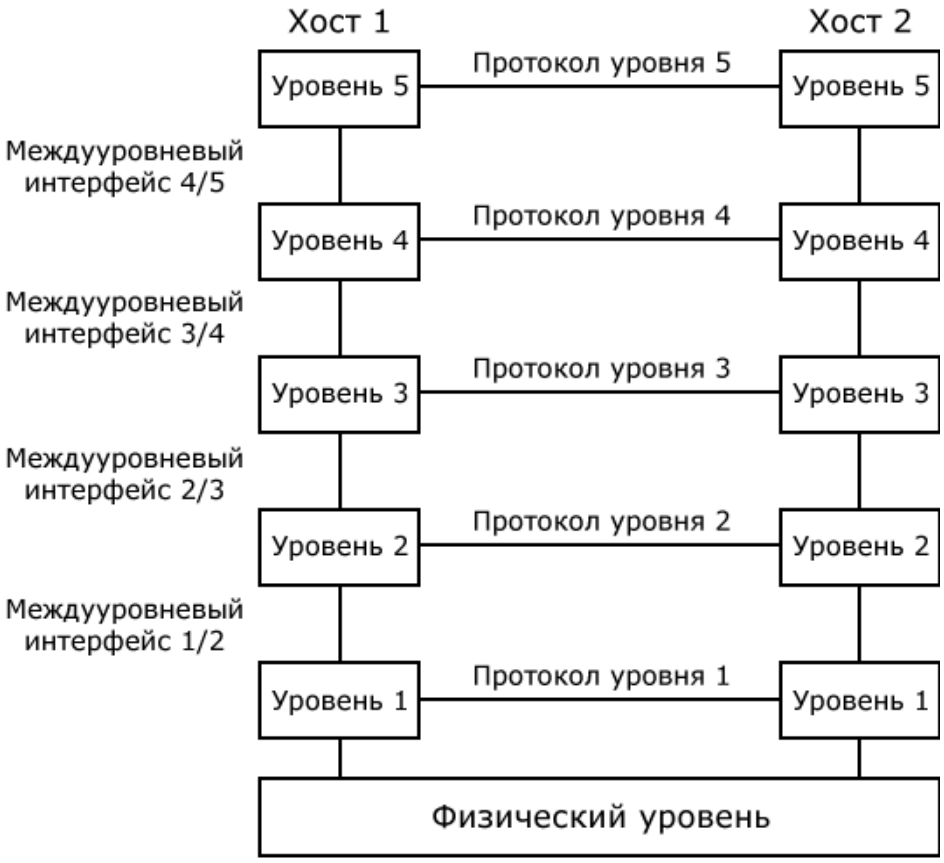


Рис. 2.1. Уровни, протоколы, интерфейсы

соответствующие уровни. Они виртуально (логически) общаются при помощи протоколов. В действительности, данные не пересылаются с уровня **n** одной машины на уровень **n** другой

машины. Вместо этого, каждый уровень машины-отправителя, начиная с верхнего, передает данные и управление уровню, лежащему ниже, пока не будет достигнут самый нижний уровень. Такие сообщения называются служебными элементами данных SDU (Service Data Unit). Ниже первого уровня находится физический носитель, по которому и производится обмен информацией. На приемной стороне пересылаемый блок данных последовательно проходит уровни машины-получателя снизу вверх. Каждый уровень выполняет свою группу функций, необходимых для приема данных.

Между каждой парой смежных уровней *интерфейс*. Это аппаратно-программные средства, а также совокупность правил, которые обеспечивают взаимодействие смежных уровней.

Когда разработчики сетей решают, сколько уровней следует включить в архитектуру сети и какие функции должен выполнять каждый уровень, очень важно определение ясных интерфейсов между уровнями. Необходимо, чтобы каждый уровень выполнял особый набор хорошо понятных функций. Минимизация количества служебной информации, передаваемой между уровнями, ясно разграниченные интерфейсы значительно упрощают изменение реализации уровня (например, замену телефонных линий спутниковыми каналами). При многоуровневом подходе всего лишь требуется, чтобы новая реализация определенного уровня предоставляла такой же набор услуг вышестоящему уровню, что и предыдущая.

Набор уровней и протоколов называется **архитектурой сети**. Спецификация архитектуры должна содержать достаточно информации для написания программного обеспечения или создания аппаратуры для каждого уровня так, чтобы они корректно выполняли требования протокола. Ни детали реализации, ни спецификации интерфейсов не являются частями архитектуры, так как они спрятаны внутри машины и не видны снаружи.

Чтобы проще понять суть многоуровневого общения, можно воспользоваться следующей аналогией (рис. 2.2).

Рис. 2.2. Пример многоуровневого общения

Представим, что существуют два абонента Боб и Алиса (уровень 3), один из них говорит на английском языке, а другой – на французском. Поскольку нет общего языка, на котором они могут общаться непосредственно, каждый из них использует переводчика (одноранговые процессы уровня 2). Каждый из переводчиков, в свою очередь, нанимает секретаря (одноранговые процессы уровня 1). Боб желает сказать своему собеседнику «Я люблю Вас». Для этого он передает сообщение на английском языке по интерфейсу 2/3 (интерфейс, находящийся между вторым и третьим уровнем) своему переводчику. Переводчики договорились общаться на нейтральном языке – русском. Таким образом, сообщение преобразуется к виду «Я люблю Вас». Выбор языка является протоколом второго уровня и осуществляется одноранговыми процессами уровня 2. Затем переводчик отдает сообщение секретарю для передачи, например, по факсу (протокол первого уровня). Когда сообщение получено другим секретарем, оно переводится на французский язык и через интерфейс 2/3 передается абоненту Алисе. Заметим, что каждый протокол полностью независим, поскольку интерфейсы одинаковы с каждой стороны. Переводчики могут переключиться с русского языка, скажем, на финский, при условии, что оба будут согласны. При этом в интерфейсах второго уровня с первым или с третьим уровнем ничего не изменится. Подобным образом секретари могут сменить факс на электронную почту или телефон, не затрагивая (и даже не информируя) другие уровни. Каждое изменение касается только обмена информацией на своем уровне. Эта информация не будет передаваться на более высокий уровень.

Рассмотрим технический пример: как обеспечить общение для верхнего уровня

пятиуровневой сети (рис. 2.3). Сообщение М создается приложением, работающим на уровне 5, и передается уровню 4 для передачи. Уровень 4 добавляет к сообщению заголовок (34), например, для идентификации номера сообщения, и передает результат уровню 3. Во многих сетях сообщения (данные), передаваемые на уровне 4, не ограничиваются по размеру, однако почти всегда подобные ограничения накладываются на протокол третьего уровня. Соответственно, уровень 3 должен разбить входящее сообщение на более мелкие единицы – пакеты, предваряя каждый пакет заголовков уровня 3 – 331(для М1) и 332 (для М2). В данном примере сообщение М разбивается на две части М1 и М2. Заголовок 331 и 332 включают управляющую информацию, например, последовательные номера, позволяющие уровню 4 принимающей машины доставить сообщения своему приложению в правильном порядке, если на нижних уровнях произойдет нарушение этой последовательности. На некоторых уровнях заголовки также включают в себя размеры пересылаемых блоков данных, время пребывания в сети и другие управляющие поля.

Уровень 3 решает, какую из выходных линий использовать, то есть определяет направление дальнейшей передачи, и передает пакеты уровню 2.

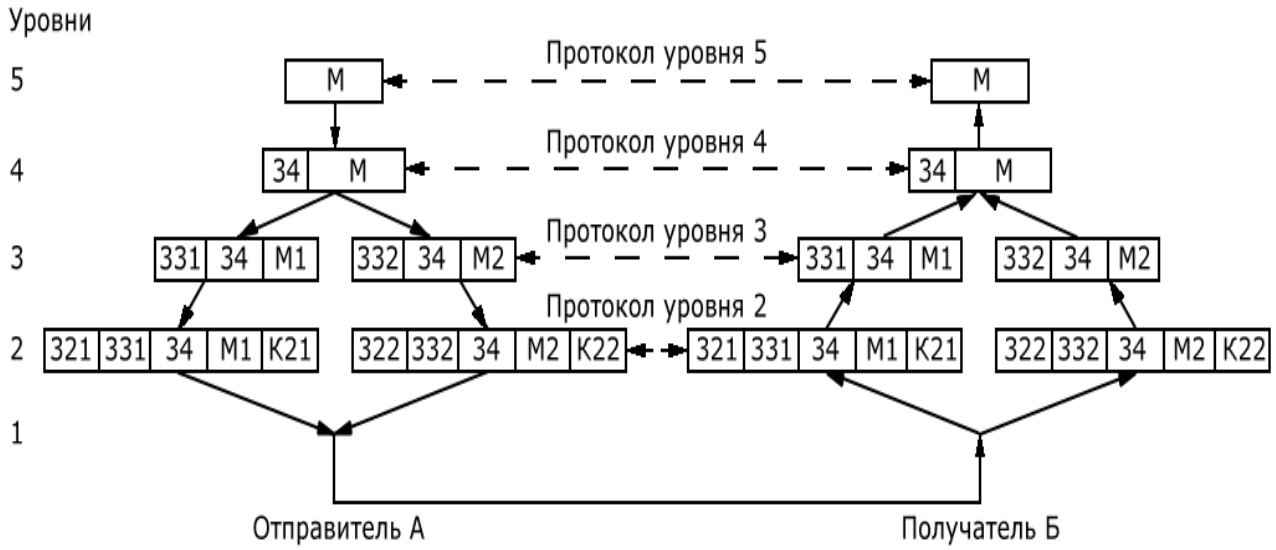


Рис. 2.3. Пример пятиуровневой сети

Здесь рассматривается разделение нагрузки, когда часть соединения М передается по одному каналу, а другая часть по другому каналу. Уровень 2 добавляет не только заголовки 321 и 322 к каждому пакету, но также и концевики К21 и К22 – завершители пакета. Заголовки и

концевики уровни 2 служат для обнаружения искаженных в канале пакетов и повтора их с буфера. Пакеты уровня 2 передаются уровню 1 для физической передачи. На приемной машине сообщение передается по уровням вверх, при этом заголовки убираются на каждом уровне по мере продвижения сообщения. Заголовки нижних уровней более высоким уровням не передаются.

Необходимо понять соотношение между виртуальным и реальным общением и разницу между протоколом и интерфейсом. Одноранговые процессы уровня 4, например, воспринимают свое общение горизонтальным, использующим протокол 4-го уровня. У каждого из них имеется процедура с названием вроде «Передать на противоположную сторону» или «Принять от противоположной стороны». На самом деле эти процедуры общаются не друг с другом, а с нижними уровнями при помощи интерфейсов 3/4. Абстракция одноранговых процессов является ключевой для проектирования сетей. С её помощью чрезвычайно трудно выполнимая задача разработки целой сети может быть разбита на несколько меньших, и вполне разрешимых проблем, а именно, разработки индивидуальных уровней.

Приведенный выше пример относится к надежной службе на основе установления соединения между пользователями. В следующем разделе рассмотрим примеры предоставления услуг с установлением и без установления соединения, надежные и ненадежные.

2.2. Службы с установлением и без установления соединений, надежные и ненадежные соединения

Уровни могут предлагать вышестоящим уровням услуги двух типов: с наличием или отсутствием установления соединения. В технике связи процедура обмена сообщениями в процессе установления или разъединения соединений называется *сигнализацией* (signaling).

Типичный пример сервиса с установлением соединения является телефонная связь: абонент сначала устанавливает соединение, разговаривает, а затем разрывает соединение. Подобное может быть и при передаче данных. В некоторых случаях отправляющая запрос сторона согласовывает параметры качества обслуживания, а другая отвергает или принимает. Примером отсутствия установления соединения является рассылка рекламы по электронной почте. Как в случае с установлением соединения, так и в случае отсутствия соединения, служба может быть надежной и ненадежной. Надежная служба обеспечивает отправку данных без потерь.

Надежная служба реализуется с помощью подтверждений, посылаемых получателем в ответ на каждое принятое сообщение. Пример надежной службы – передача файлов, которая обеспечивает доставку без искажений. Не для всех приложений годится надежная служба (например, для передачи речевой или видеоинформации – для них недопустима большая задержка из-за повторной передачи принятых с искажениями данных). Режим без подтверждений и без установления соединений называется дейтаграммным. По аналогии с телеграфом отправителю не предоставляется подтверждение о получении телеграммы. Дейтаграммный режим используется кроме передачи речи и видео также тогда, когда надежная доставка данных обеспечивается протоколами более высоких уровней.

2.3. Пакетная коммутация

В соответствии с законом «О связи» от 18 июня 2003 года [1] для сетей связи общего пользования стратегическим направлением является коммутация пакетов.

При коммутации пакетов сообщение пользователя разбивается в оконечном узле связи на пакеты - элементы сообщения, снабженные заголовком. Например, в сети **X.25** максимальная длина поля данных пакета устанавливается по согласованию (по умолчанию принимается равной 128 байт).

В заголовке пакета устанавливается адресная информация, необходимая для доставки пакета в оконечное устройство получателя. В сети X.25 используется формат адресации, определенный в рекомендации ITU-T X.121, содержащий код зоны (всего в мире 7 зон), код определенной сети в зоне и номер сетевого терминала из десяти цифр. На рис. 2.4 показана передача сообщения абонента a_i абоненту a_j. Абонент a_i подключён к центру коммутации A, а абонент a_j к центру коммутации D. Перед передачей сообщение разбивается на три пакета, которые поступают получателю через транзитные центры коммутации B и C.

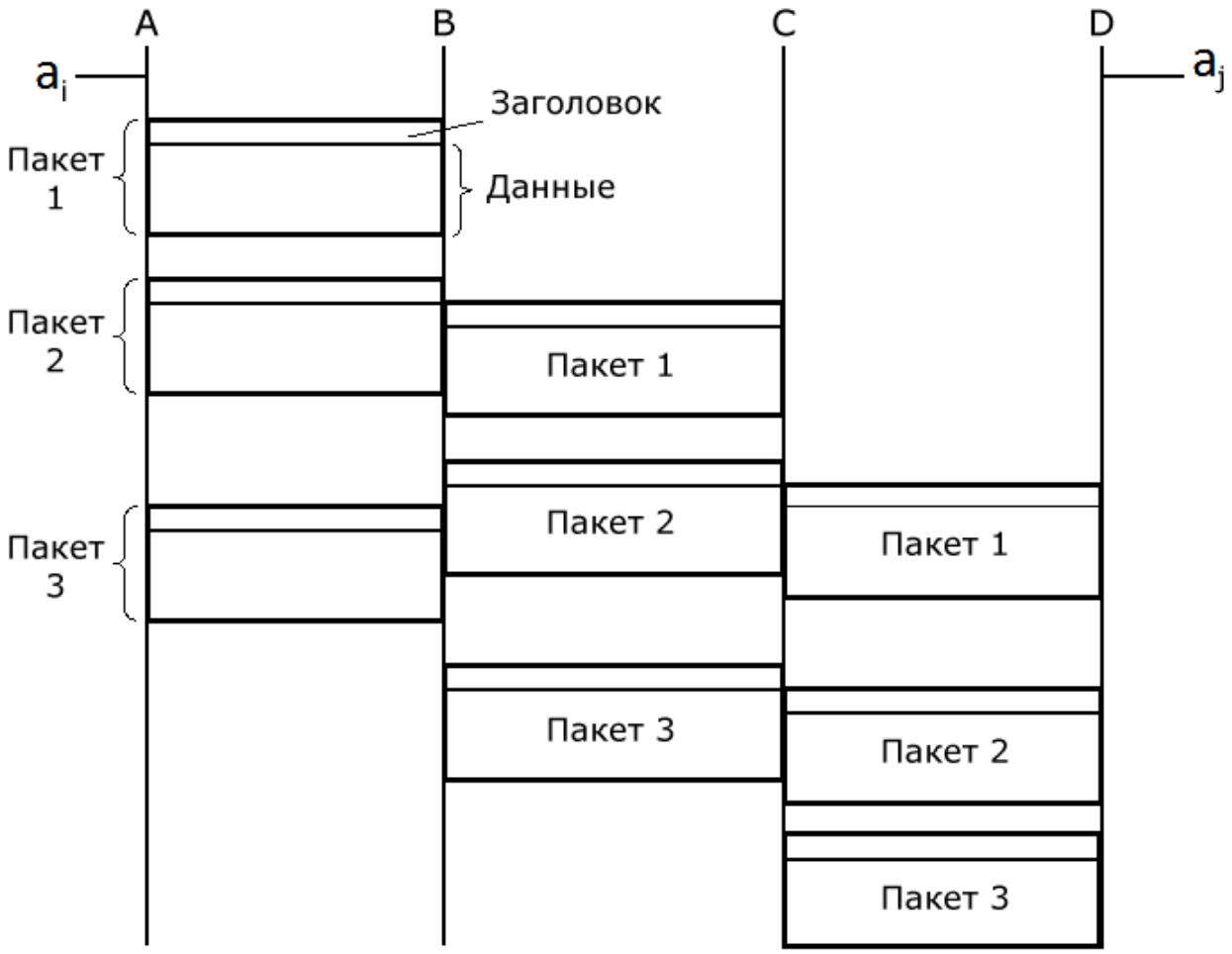


Рис. 2.4. Передача данных в сети КП

К сетям с коммутацией пакетов относится не только сеть X.25, но и более современные технологии (сети Frame Relay, ATM), а также Интернет. Пропускная способность канала в сети КП при неравномерном трафике существенно выше, чем в сетях КК. Один и тот же физический канал используется для обслуживания многих абонентов, поочередно предоставляя свою пропускную способность разным соединениям абонентов. Наибольший эффект от КП достигается при высоком коэффициенте пульсации трафика пользователей сети.

Коэффициент пульсации трафика отдельного пользователя сети определяется как отношение пиковой скорости на каком-либо коротком интервале времени к средней скорости обмена данными на длинном интервале времени и может достигать значений 100:1. Если использовать коммутацию каналов, то большую часть времени канал будет простаивать. В то же время часть ресурсов сети остается закрепленной за данной парой абонентов и недоступна другим пользователям сети.

На рис. 2.5 приведен пример мультиплексирования пакетов разных информационных потоков в одном физическом канале.

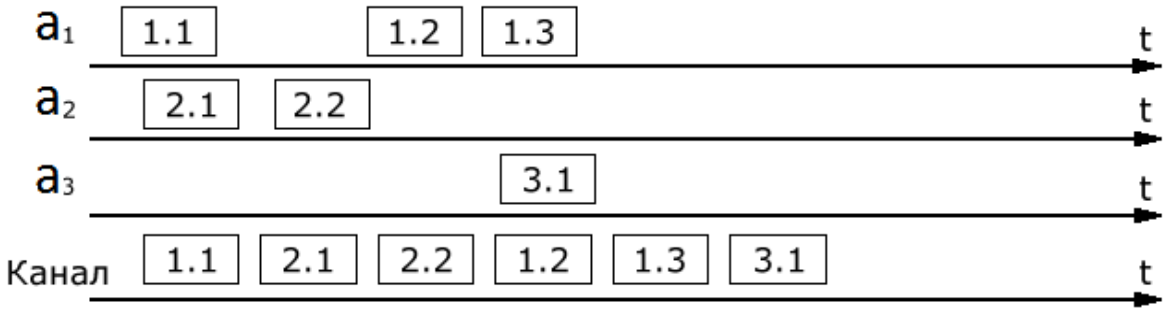


Рис. 2.5. Пример мультиплексирования пакетов в одном физическом канале

На первых трех осях изображены потоки пакетов, генерируемых абонентами а1, а2, а3. Двойная нумерация пакетов на рис. 5 обозначает номер абонента и номер пакета в потоке. Канал используется для обслуживания трех абонентов – путем разделения по времени, т.е. поочередного предоставления канала абонентам. Один канал может обеспечить работу многих взаимодействующих абонентов. Таким образом, пакет поэтапно, с переприемом, передается через ряд узлов в пункт назначения. Пакеты могут иметь переменную длину, но в достаточно узких пределах: от 50 до 1500 Байт. Пакеты транспортируются в сети, как независимые информационные блоки и собираются в сообщение в узле назначения. Коммутаторы пакетной сети имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора занят передачей другого пакета.

2.4. Стек протокола сети пакетной коммутации стандарта X.25

Рассмотрев многоуровневый принцип построения сети, перейдем к стеку протоколов (или уровней) конкретной сети пакетной коммутации стандарта **X.25.**

Изучение стека протоколов именно этой сети объясняется следующими причинами.

- Рекомендации МСЭ-Т X.25 и родственные с ней (X.3, X.28, X.75, X.121 и др.) наиболее полно соответствуют стандартизированной МСЭ-Т эталонной модели взаимодействия открытых систем (**OSI**, Open System Telecommunication), включающей 7 уровней. Следует отметить, что модель OSI не полностью отражают архитектуру построения современных технологий сетей связи. Несмотря на это модель OSI является прекрасным механизмом для анализа основ архитектуры этих сетей [8].
- Многие из современных технологий имеют корни в стандарте X.25. Сети X.25

продолжают находится в эксплуатации (в том числе и в России – сеть общего пользования «РОСПАК» и др.).

- Изложение принципов программного обеспечения в сети X.25 позволяет изучить процедуры функционирования технологий более современных сетей (Frame Relay, ATM, IP-сети, ОКС№7, MPLS).
- Для классификации сетей связи используются различные признаки. Чаще всего сети делятся по величине территории, которую покрывает сеть. Причиной является отличие технологий локальных и глобальных сетей. Глобальные сети, к которым относятся сети X.25, предназначены для обслуживания большого количества абонентов, разбросанных на большой территории – в пределах региона, страны, континента или всего земного шара. Услугами глобальной сети могут пользоваться локальные сети предприятий или отдельные компьютеры. Исторически глобальные сети появились первыми, хотя технология их значительно сложнее. Именно при их построении были впервые отражены основные концепции сетей, такие как многоуровневое построение коммуникационных протоколов, технология коммутации пакетов, требования к качеству обслуживания QoS (Quality of Service) и соглашение о гарантии обслуживания SLA (Service Level Agreements).

На рис. 2.6 представлен стек протоколов сети X.25.

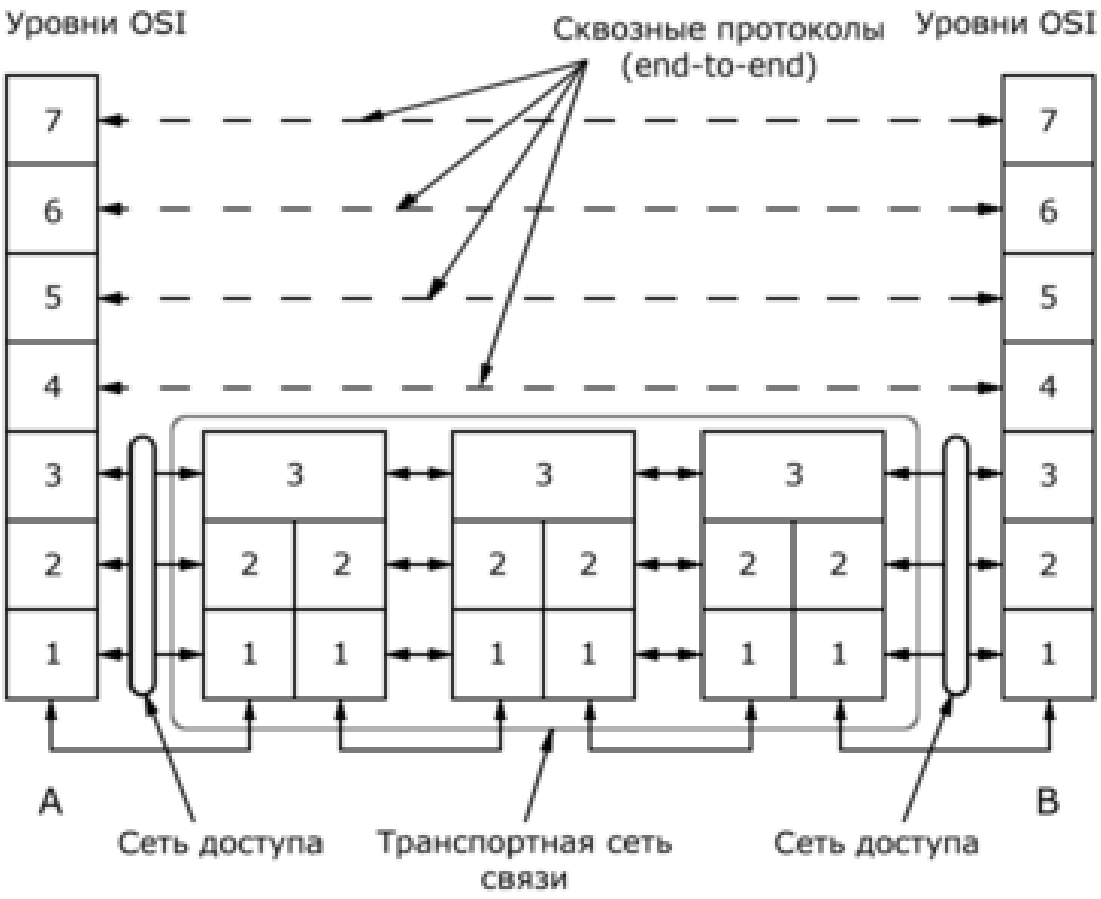


Рис. 2.6. Стек протоколов сети пакетной коммутации X.25

Здесь показана транспортная сеть, состоящая из трех *центров коммутации пакетов* **ЦКП** (**ЦКП1**, **ЦКП2**, **ЦКП3**) и двух оконечных станций - A и B. ЦКП включает три нижних уровня, соответствующих модели OSI:

- физический уровень (уровень 1), осуществляющий передачу бит;
- канальный уровень или уровень звена данных X.25/2 (уровень 2), осуществляющий свободную от ошибок передачу по отдельному каналу связи;
- сетевой уровень X.25/3 (уровень 3), обеспечивающий маршрутизацию (коммутацию) сообщений по каналам, связывающим ЦКП.

На этих уровнях действуют протоколы транспортной сети между ЦКП и протоколы доступа к сети. Как правило, протоколы верхних уровней модели OSI (с 4 по 7) реализуются только на оконечных устройствах сети и являются сквозными протоколами.

Четвертый уровень в модели OSI является транспортным уровнем. Транспортный уровень располагается на оконечных станциях и обеспечивает интерфейс между транспортной сетью

(ЦКП1, ЦКП2, ЦКП3) и верхними тремя уровнями обработки данных, размещенными у пользователя. Транспортный уровень, в частности, выполняет сегментирование данных, передаваемых в сеть, в случае необходимости.

К уровням обработки данных, которые иногда называют уровнями приложения, относятся прикладной, представительный и сеансовый уровни. Прикладной уровень обеспечивает поддержку прикладного процесса пользователя и отвечает за семантику, то есть смысловое содержание сообщений, которыми обмениваются машины отправителя и получателя. На прикладном уровне находятся сетевые приложения: электронная почта, передача файлов по сети и пр.

Представительный уровень или уровень представления определяет синтаксис передаваемых сообщений, то есть, набор символов алфавита и способы их представления в виде двоичных чисел (первичный код). Уровень обеспечивает процесс согласования различных кодировок, а также может выполнять шифрование, дешифрование и сжатие данных. Уровень представления обеспечивает прикладному процессу независимость от различий в синтаксисе. Сеансовый уровень управляет сеансами взаимодействия прикладных процессов пользователей. Сеанс создается по запросу процесса пользователя, переданному через прикладной и представительный уровни. На этом уровне определяется, какая из сторон является активной в данный момент, и обеспечивается синхронизация диалога. Средства синхронизации позволяют организовывать контрольные точки в длинных передачах, чтобы в случае отказа можно было вернуться к последней контрольной точке, не начиная всю передачу данных сначала.

На рис. 2.7 показан перенос данных в сетях ПК X.25 через все уровни оконечных устройств абонентов А и Б, а также нижние три уровня узлов транспортной сети. Здесь приняты обозначения D3, D4, D5, D6, D7 - блоки данных уровней соответственно уровней 3, 4, 5, 6, 7. Обозначения З2, З3, З4, З5, З6 – заголовки блоков данных соответственно уровней 2, 3, 4, 5, 6. Передача данных физически производится по вертикали: на передачу с верхнего уровня на нижний и на приёме наоборот. Для передачи сообщения четвертого уровня оконечного устройства (состоящего из заголовка З4 и данных Д5) оно вкладывается (*инкапсулируется*) в пакет третьего уровня (сетевого). При этом к пакету добавляется заголовок З3 (включающий адрес). На основе адресов заголовка производится коммутация в центре коммутации пакетов. Далее производится инкапсуляция этого пакета в кадр второго уровня. Как видно из рисунка, кроме заголовка З2 в кадр добавляется концевик К2, который служит для обнаружения на приёме искаженного в канале кадра.

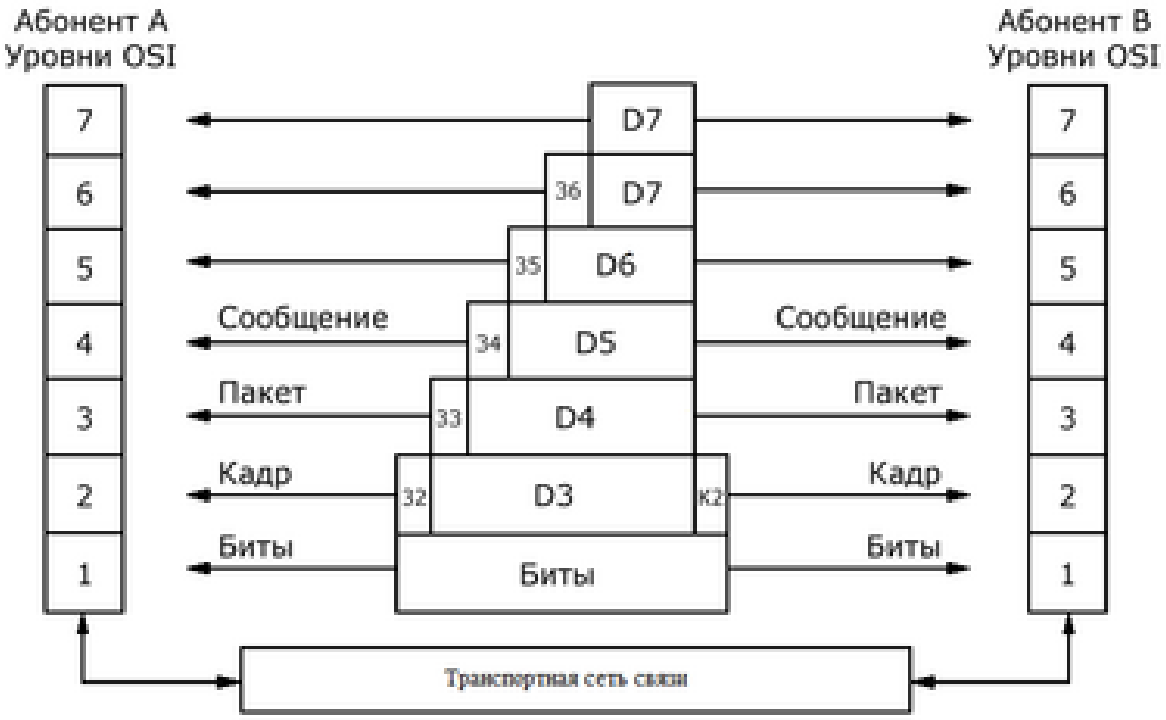


Рис. 2.7. Перенос данных в сетях ПК X.25

2.5. Шифрование сообщений в сети пакетной коммутации

Одним из способов обеспечения противодействия угрозам информационной безопасности некоторых сетей ограниченного пользования является *шифрование*. При использовании шифрования необходимо решать, что именно следует шифровать и на каком уровне эталонной модели OSI следует осуществлять защиту информации. Для таких сетей коммутация информационных пакетов производится на основании таблицы маршрутизации, включающих физические адреса. В этом отношении они отличаются от сети пакетной коммутации стандарта X.25 (подробно об этом будет изложено в главе 7) и в них предусмотрено два основных варианта шифрования: канальное и сквозное шифрование [9]. Их использование показано на рис. 2.8.

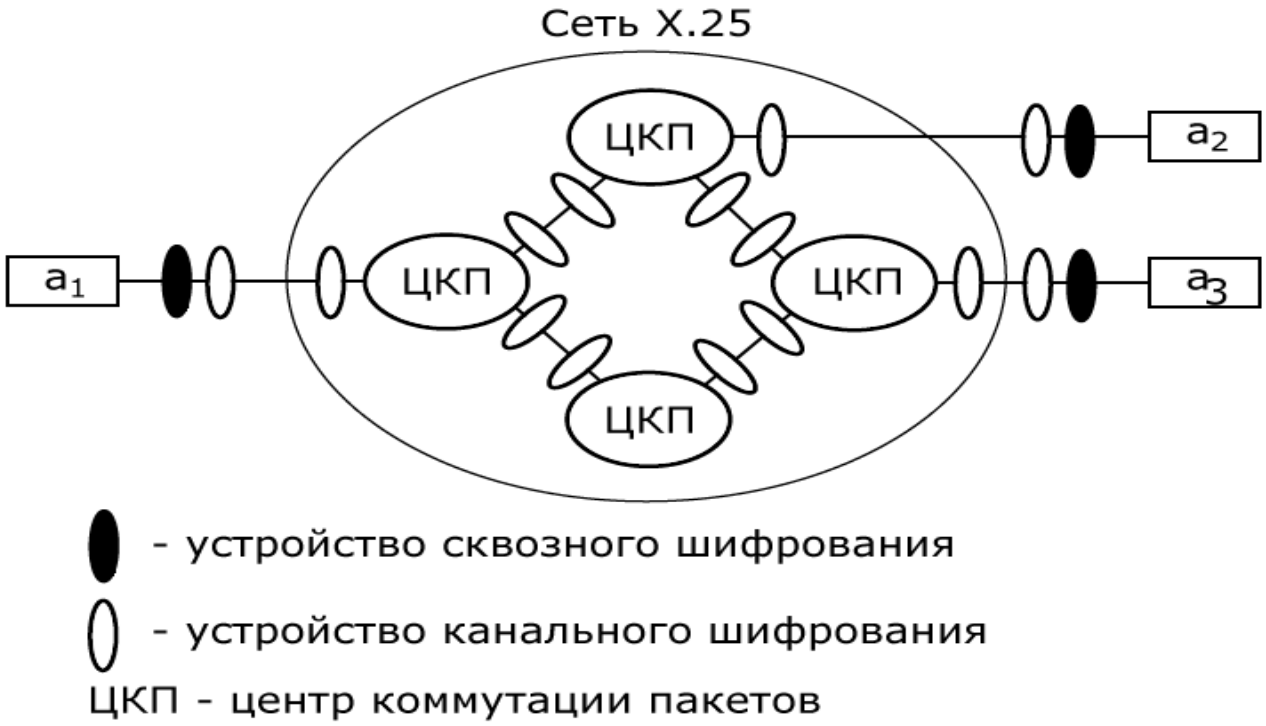


Рис. 2.8. Шифрование в сети коммутации пакетов

При *канальном шифровании* каждый уязвимый канал на третьем уровне оборудуется устройствами шифрования на обоих концах. Таким образом, весь поток данных в канале оказывается защищенным. Хотя для этого в большой сети потребуется значительное количество устройств шифрования (на каждый канал сети), преимущества такого подхода очевидны. Недостатком же является то, что сообщение должно расшифровываться каждый раз, проходя через коммутатор пакетов, поскольку коммутатор должен прочитать адрес в заголовке пакета, чтобы направить пакет по нужному направлению. Поэтому сообщение оказывается уязвимым в каждом коммутаторе.

При *сквозном шифровании* процесс шифрования выполняется на уровне выше третьего только в двух конечных станциях. Исходные данные шифруются в оконечном устройстве источника сообщений. Затем данные в шифрованном виде передаются без изменений через всю сеть получателю. Адресат использует тот же ключ, что и отправитель, и поэтому может дешифровать полученные данные. Эта схема кажется безопасной с точки зрения защиты от воздействий в канале связи или узлах коммутации пакетов. Однако и у такого подхода есть слабое место.

Какую часть каждого пакета при сквозном шифровании должен шифровать источник? Предположим, что шифрует весь пакет, включая заголовок. Но этого делать нельзя, так как выполнить расшифровку сможет только получатель. ЦКП, получивший такой пакет, не

сможет прочитать заголовок и поэтому не сумеет переслать пакет в соответствии с адресом. Отсюда следует, что отправитель должен шифровать только ту часть пакета, которая содержит данные пользователя, и оставить заголовок нетронутым.

Итак, при сквозном шифровании данные пользователя оказываются защищенными, чего нельзя сказать о самом потоке данных, поскольку заголовки пакетов передаются в открытом виде. Возможность изучения структуры потока по адресам проходящих пакетов называется анализом трафика [10]. Чтобы достичь более высокого уровня защищенности, необходима комбинация канального и сквозного шифрования, например, как показано на рис. 2.8, на котором приведена сеть коммутации пакетов с четырьмя центрами коммутации ЦКП. К трем из этих ЦКП подключены оконечные устройства a_1, a_2, a_3. Рассмотрим следующую ситуацию. Два оконечных устройства устанавливают соединение для передачи данных с использованием шифрования. Сообщения передаются пакетами, состоящими из заголовка и поля данных. Какую часть пакета должен шифровать оконечный пункт-источник сообщения?

При использовании обеих форм шифрования узел-источник шифрует на уровне выше третьего пакет данных пользователя, используя ключ сквозного шифрования. Затем весь пакет шифруется с помощью ключа канального шифрования. При движении пакета по сети каждый коммутатор сначала дешифрует пакет с применением ключа шифрования соответствующего канала, чтобы прочитать заголовок, а затем снова шифрует весь пакет для передачи его по следующему каналу. Теперь весь пакет защищен почти все время – за исключением времени, когда он находится в памяти коммутатора пакетов, где заголовок пакета оказывается открытым.

ГЛАВА 3. Физический уровень сети пакетной коммутации

3.1. Архитектура физического уровня

Физический уровень является самым нижним уровнем эталонной модели OSI и обеспечивает физическую и электрическую связь на участке абонентского доступа и в транспортной сети между узлами коммутации.

Основными топологиями физического уровня являются “точка-точка” и “точка-многоточие”. В первом варианте (рис. 3.1, а) два взаимодействующих устройства составляют одну связь. Эта связь может быть дуплексной, симплексной и полудуплексной. При дуплексной передаче обе стороны могут передавать и принимать данные когда угодно и даже делать это одновременно.

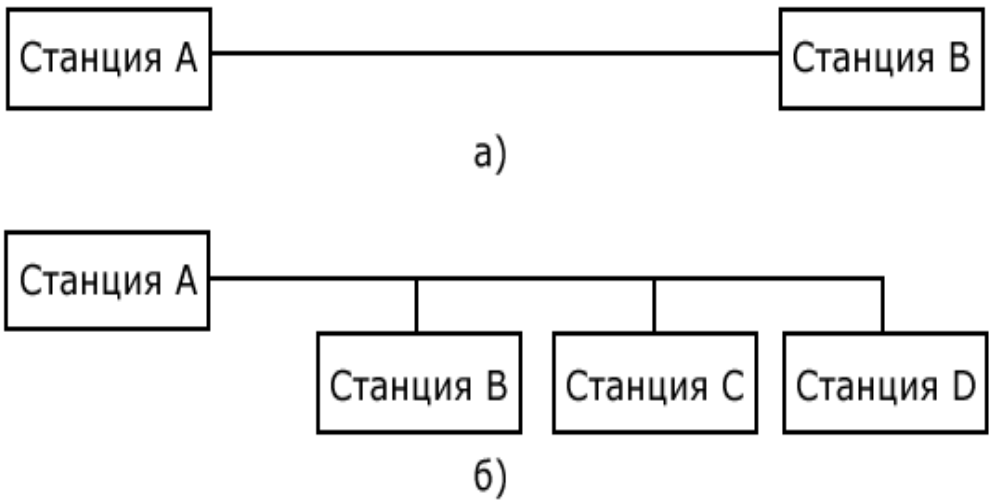


Рис. 3.1. Основные топологии физического уровня: а) “точка-точка”; б) “точка-многоточие”

При симплексной передаче одно из устройств может только передавать данные, а второе только принимать. Направление передачи никогда не может измениться. Примером может служить вещательное телевидение. При полудуплексной передаче любое из устройств может быть как передатчиком, так и приемником, но никогда не может находиться в обоих состояниях одновременно. Примером может быть *локальная вычислительная сеть* (**ЛВС**) стандарта Ethernet. В такой системе передача в одном направлении должна быть завершена, прежде чем может начаться передача в другом направлении. Вариант “точка-многоточие” (рис. 3.1, б) применяется в сотовой сети связи GSM при определении базовой станции вызываемой мобильной станции (с тем, чтобы не опрашивать поочередно все мобильные станции соты).

На рис. 3.2, a), b), c), d) приведены другие топологии физического уровня (“кольцо”,

“звезда”, “шина” и “точка-точка” параллельно по нескольким каналам), которые являются вариантами приведённых основных топологий. Возможно два варианта передачи данных между двумя станциями по нескольким каналам связи (рис. 3.2, d). В первом случае один канал является основным, а второй – резервным (в горячем резерве). В этом случае передача всех данных осуществляется по основному каналу, а при его неисправности по резервному. Во втором случае производится передача параллельно по двум каналам либо одних и тех же данных, либо с разделением нагрузки (часть данных станции передаётся по одному каналу, а часть по-другому). Это обеспечивает более высокую скорость передачи. В случае передачи с разделением нагрузки при неисправности одного из каналов все данные станции передаются по оставшемуся каналу.

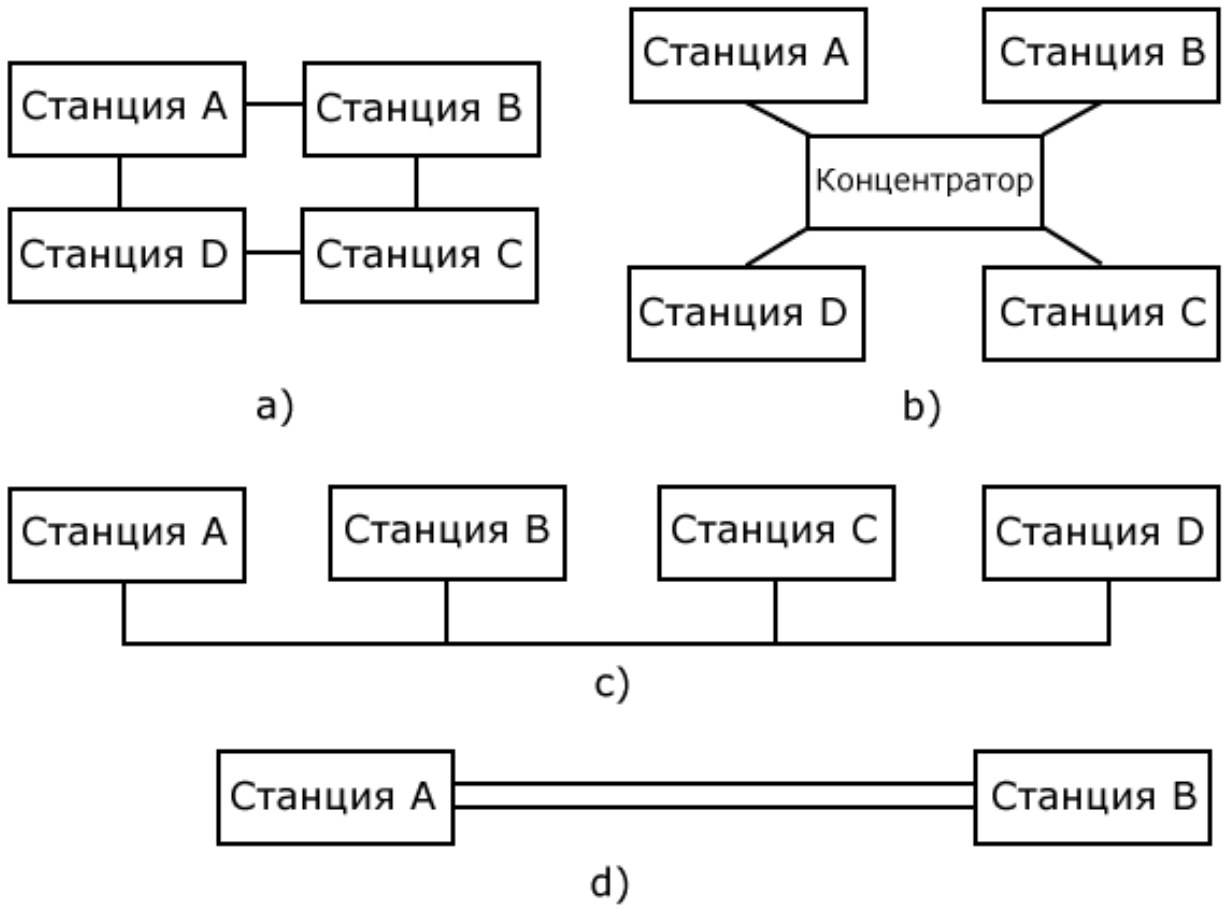


Рис. 3.2. Топологии физического уровня: а) “кольцо”, “б) звезда”, с)“шина” и d)“точка-точка”

3.2. Физическая среда передачи информации

На физическом уровне в современных технологиях сетей применяется одни из четырех

типов среды передачи:

- металлический симметричный кабель с медными жилами, состоящий из различного числа “витых пар”;
- коаксиальный кабель (подобный кабелю, используемому в телевизионных сетях с антенной общего пользования);
- волоконно-оптический кабель;
- окружающее пространство (используется при организации беспроводной передачи данных).

Рассмотрим кратко характеристики физической среды передачи данных с точки зрения пропускной способности и помехозащищенности.

Кабель “витая пара” состоит из двух изолированных проводников, перевитых между собой. Помехозащищенность пары выше, чем если бы два проводника не были скручены. По сравнению с другими средами передачи данных помехозащищенность и пропускная способность меньше.

По сравнению с “витой парой” коаксиальный кабель позволяет большую пропускную способность и обладает большей помехозащищенностью.

Оптоволоконный кабель изготавливается из кварцевого стекла и передача в нем осуществляется не электронами, а световой волной. Волоконно-оптический кабель имеет большое преимущество перед всеми остальными кабелями как в части пропускной способности (до нескольких Терабит в секунду), так и в части помехозащищенности.

Первичная сеть представляет собой совокупность каналов и трактов передачи, образованных оборудованием узлов и линий передачи, соединяющих эти узлы.

Следует отметить большое количество устаревшей техники связи России, использующей симметричный и коаксиальный кабели. Эти кабели известны не только более низкими показателями пропускной способности и помехозащищенности по сравнению с волоконно-оптическими кабелями, но и дороговизной по многим показателям (прокладка, обслуживание и др.). На первичных сетях продолжают использовать линии связи, построенные на металлических кабелях, симметричных кабелях в свинцовой, алюминиевой или стальной оболочках с емкостью, в основном, четыре и семь четверок с медными жилами диаметром 1,2 мм. С 1996 года в России все новое строительство междугородних и международных линий связи осуществляется на волоконно-оптических кабелях.

Система спутниковой связи России играет важную роль в организации каналов связи для междугородных сетей связи (особенно в труднодоступных и удаленных регионах страны).

3.3. Аналоговая и цифровая связь

Существует *аналоговая* и *цифровая связь*. Аналоговые сигналы распространяются по линиям связи в виде непрерывно меняющихся синусоидальных электромагнитных волн, которые характеризуются частотой, фазой и амплитудой. На рис. 3.3 приведен один период такого синусоидального колебания 1 Гц.

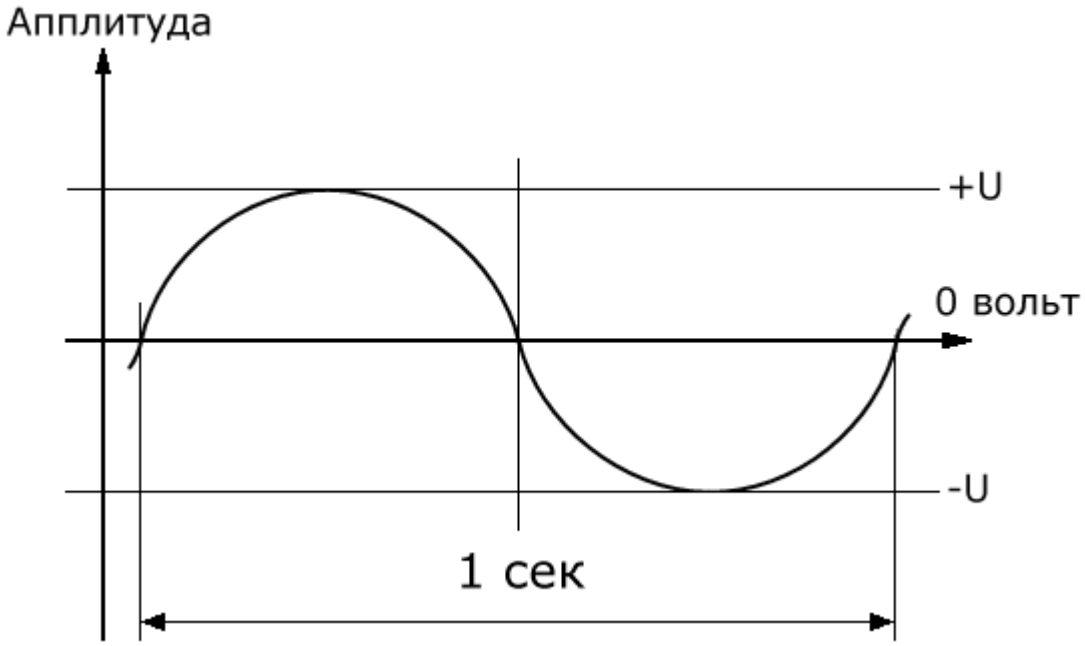


Рис. 3.3. Синусоидальная волна с частотой 1Гц

Волна, которая, например, 10 раз в течение одной секунды проходит через максимум (+U вольт) имеет частоту 10 Гц. Полоса, в которой распределяются звуковые сигналы (голос) между абонентами аналоговой связи по телефонной сети общего пользования ТфОП составляет 3100Гц (диапазон 300-3400Гц). Такой канал называется каналом тональной частоты. В случае необходимости высококачественного воспроизведения речи и музыкальных программ (на уровне радиовещательных сигналов) требуется увеличение полосы до 10кГц и выше.

На рис. 3.4 приведена амплитудно-частотная характеристика канала тональной частоты.

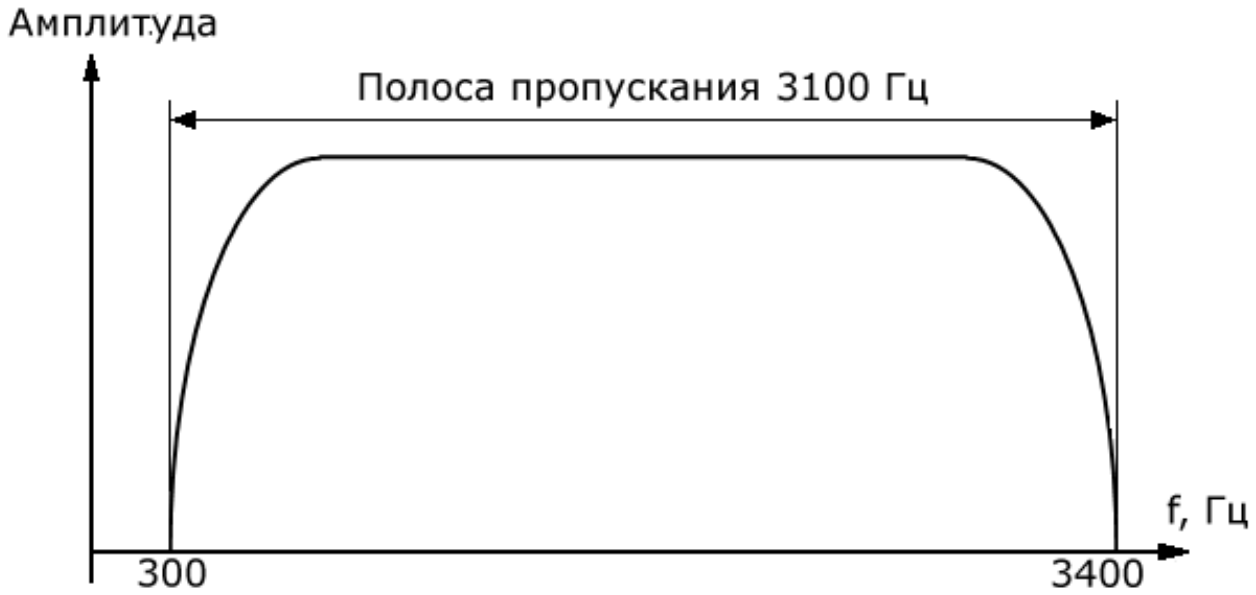


Рис. 3.4. Амплитудно-частотная характеристика канала тональной частоты

На рис. 3.5 приведены две синусоидальные волны с разными частотами (рис. 3.5, а) и фазами (рис. 3.5, б).

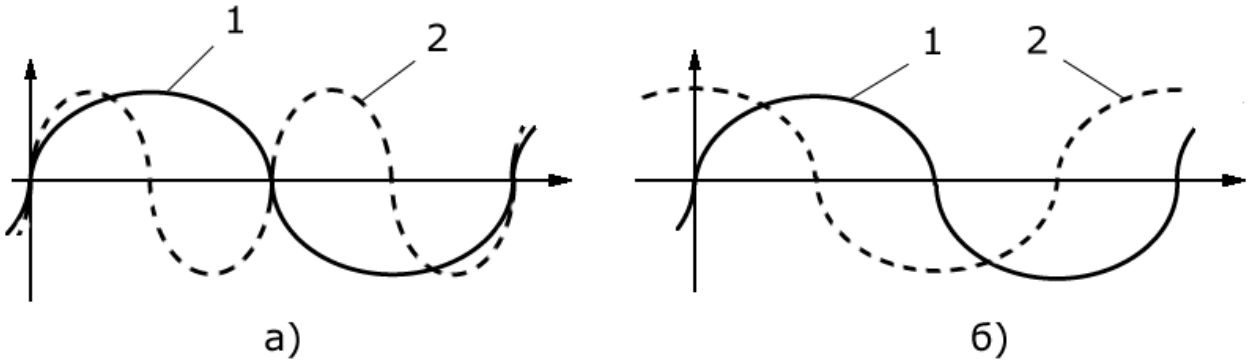


Рис. 3.5. Синусоидальные волны с разными частотами и фазами

Цифровая связь осуществляет передачу сообщений с помощью битов. Как аналоговым, так и цифровым сигналам присуща нестабильность при передаче. Оба сигнала с увеличением дальности распространения ослабевают, затухают и подвергаются воздействию помех. Однако цифровые сигналы поддаются коррекции и восстановлению лучше, чем аналоговые. Из рисунка 3.6 видно, что когда цифровой сигнал, подвергающийся воздействию

помехи, начинает затухать, предназначенное для его усиления устройство на линии связи без искажений восстанавливает сигнал (т.е. единицу или нуль). Помеха отбрасывается, а не регенерируется и не усиливается, как в случае с аналоговым сигналом.

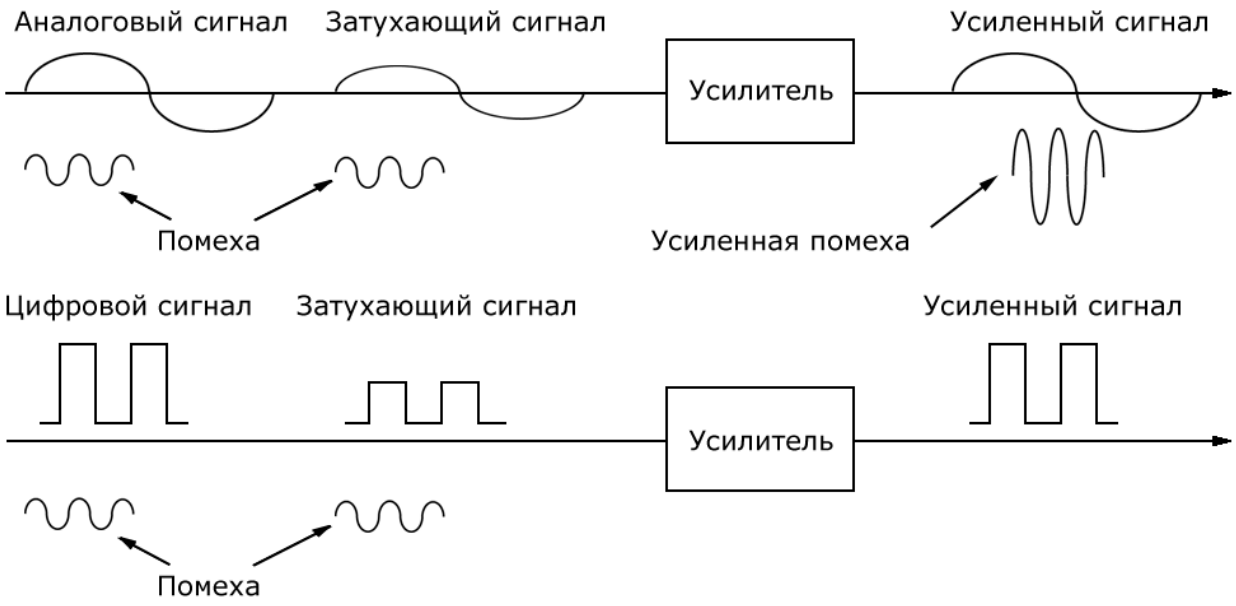


Рис. 3.6. Усиление помехи в аналоговых линиях и устранение ее в цифровых линиях

Помимо чистоты передачи аудиосигналов, цифровая связь обеспечивает пересылку данных с меньшим числом ошибок. В аналоговых линиях, где происходит усиление и сигнала помехи, принимающие устройства могут интерпретировать этот сигнал как бит информации. В цифровой связи сигнал помехи отбрасывается и поэтому искажения и ошибки при передаче данных наблюдаются реже.

Хотя аналоговая связь, имеет недостатки перед цифровой связью (сложнее оборудование, больше вероятность ошибок, ниже скорости передачи, хуже чистота звуков), много оборудования местных *телефонных сетей общего пользования* России остается на аналоговых линиях.

3.4. Модем и цифровая абонентская линия ADSL

Для передачи двоичной информации (бит) по аналоговым каналам используются модемы, установленные между компьютером и аналоговой линией. Рассмотрим принцип работы модема. Применяемая в них модуляция используется не только для передачи данных по каналам тональной частоты, но и:

- в высокоскоростном канале абонентского доступа ADSL и др.;
- в мобильных сетях GSM, EDGE, Wi-Fi, WiMAX, UMTS.

В сетях передачи данных по каналам тональной частоты и на участке абонентского доступа в цифровых абонентских **xDSL** модемы служат для выполнения двух функций:

- преобразования цифровых сигналов в аналоговые и обратно (модуляция и демодуляция);
- увеличение скорости передачи.

В некоторых из перечисленных сетей связи ограничиваются только первой функцией. Работа модема в канале тональной частоты построена на модуляции (*амплитудной*, *частотной* и *фазовой*) непрерывной синусоидальной несущей частоты от 1000 до 2000Гц.

При *амплитудной* модуляции используются различные значения амплитуды синусоидальной несущей частоты. В качестве синонима “модуляции” часто используется термин “манипуляция”. При *частотной* модуляции используется несколько различных частот синусоидальной несущей, а при *фазовой* модуляции – несколько сдвигов фаз на постоянный угол. Для реализации модемов делается 2400 или 4000 отсчетов в секунду. За каждый отсчет передается один символ, который может выражать один или несколько бит цифрового сигнала. Число отсчетов в секунду измеряется в бодах. Если при амплитудной модуляции символ может принимать одно из двух значений амплитуды синусоидальной несущей, то цифровая скорость составляет 2400 бит/с. Если каждый символ может принимать четыре значения (выраженные двумя битами), то цифровая скорость составляет 4800 бит/с при той же линии 2400 бод. То же самое происходит, если менять не амплитуду, а частоту или фазу.

Битовой скоростью называется объем информации, передаваемой по каналу за секунду. Битовая скорость равна произведению числа символов на число бит на один символ.

Модемы часто используют комбинированный метод модуляции сигналов. Одним из них является комбинация амплитуды и фазовых сдвигов.

На рис. 3.7 изображен комбинированный метод модуляции, использующий 16 комбинаций - 4 комбинации амплитуды и 12 комбинаций фазовых сдвигов. Такая схема называется квадратурной амплитудной модуляцией или **QAM-16** (Quadrature Amplitude Modulation) использующей 4 бита на символ. Такой модем позволяет по линии с пропускной способностью 2400 бод передавать с скоростью 9600 бит/с.

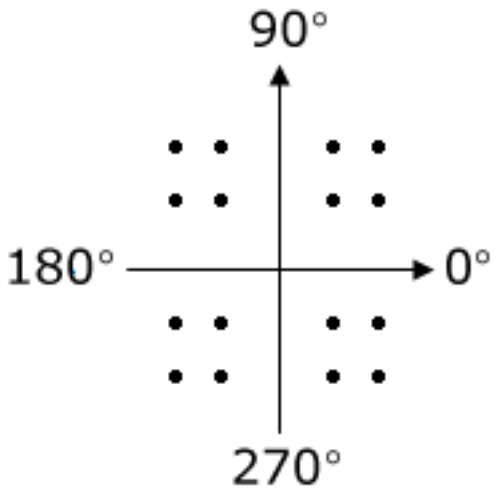


Рис. 3.7. Комбинированный метод модуляции QAM-16

Чем больше точек находится на амплитудно-фазовой диаграмме, тем больше вероятность воздействия помех (**шума**) при детектировании амплитуды или фазы, т.е. искажения бита. Для уменьшения вероятности такого воздействия были разработаны стандарты, предусматривающие включение в состав каждого отсчета дополнительные биты коррекции. Так, например, стандарт **ITU-T V.32** предусматривает 32 точки на диаграмме для передачи 4 бит/символ и 1 контрольный бит (т.е. всего 5 бит на символ).

Согласно теореме Найквиста-Котельникова для канала с диапазоном частот f максимальное число отсчетов в секунду равно 2f. Стандарт V.32 предоставляет пользователю максимальную скорость передачи данных по каналу тональной частоты 64000 бит/с. При этом максимальное число отсчетов в секунду – 8000, а число бит на отсчет равно 8. В США 1 бит является контрольным, что позволяет работать с битовой скоростью 56000 бит/с. Эти скорости предоставляются модемом при передаче от сети абоненту. В обратную сторону скорость 33,6 Кбит/с. В Европе все 8 бит являются информационными, поэтому, в принципе, максимальная скорость может быть 64 Кбит/с, однако международным соглашением

установлено ограничение в 56 Кбит/с.

Телефонные компании разработали так называемые множества широкополосных цифровых абонентских линий, носящие общее название **xDSL** (Digital Subscriber Line). Одной из них является **ADSL** (Asymmetric DSL – асимметричная DSL). На существующих местных (т.е. городских и сельских) линиях ADSL предоставляет работу отдельно по телефону и по передаче данных с битовой скоростью, значительно превышающей 56 Кбит/с.

В ADSL на передачу отводится не диапазон в 3100 Гц, выделяемый на АТС фильтром, а весь спектр местной линии, который составляет примерно 1,1 МГц. Весь этот диапазон частот разделен на 256 независимых каналов, одни из которых отводится под телефонную связь, а 5 каналов не используются. Из оставшихся 250 каналов одни занят контролем передачи в сторону провайдера, один – в сторону пользователя, а 248 доступны для передачи данных. Провайдер может самостоятельно определить сколько каналов использовать под исходящий трафик, сколько под входящий.

В каждом канале используется метод квадратурной амплитудной модуляции **QAM**, количество бит на бод достигает при этом 15 (скорость отсчета 4000 бод), а амплитудно-фазовая диаграмма аналогична представленной на рис. 3.7. Пропускная способность входящего трафика при отведенных для него 224 каналах составляет 13,44 Мбит/с. Помехи в каналах связи не позволяют достигнуть такой скорости, однако 8 Мбит/с на коротких качественных линиях – это реально.

Приведем в качестве примера (для канала с определенным качеством) соответствие между скоростями передачи и расстоянием от абонента до телефонного узла.

- 5,5 км 1,544 Мбит/с,
- 4,9 км 2,048 Мбит/с,
- 3,7 км 6,312 Мбит/с,
- 2,7 км 8,448 Мбит/с.

С появлением первых ADSL-модемов, провайдеры увидели перспективность данной технологии и начали использовать её для предоставления доступа к сети Интернет. Несмотря на появление более быстрых беспроводных технологий доступа WiFi, WiMAX, LTE (которые подлежат рассмотрению в следующих главах) технология ADSL по-прежнему актуальна для крупных городов, имеющих развитую инфраструктуру проводной связи. В ряде европейских стран ADSL является стандартом де факто при обеспечении населения достаточно быстрым и недорогим интернетом. Так, в Финляндии, где каждому жителю страны законодательством с

июня 2010 г. гарантирован доступ в интернет, подключение большинства домов производится именно по технологии ADSL.

Скорость потока данных от пользователя на телефонный узел в диапазоне от 16 до 640 Кбит/с. Возможны и другие виды модуляции. В сетях связи используется также фазовая модуляция - бинарная фазовая модуляция BPSK (Binary Shift Keying), при которой фаза меняется на 180^o при изменении бита данных.

3.5. Аналого-цифровое преобразование

Выше мы познакомились с преобразованием дискретной формы представления информации в аналоговую. Рассмотрим обратную задачу – преобразование и передача аналоговой информации в дискретной форме (в виде цифровых сигналов). Такая задача была решена, когда речевые сообщения стали передаваться по телефонным сетям в виде последовательности единиц и нулей, что повышает качество передаваемой речи, увеличивает скорость передачи, уменьшает вероятность ошибок в каналах связи. На рис. 3.8 показан принцип работы аналого-цифрового преобразователя.

Преобразование непрерывного аналогового звукового сигнала в цифровой сигнал называется дискретной модуляцией аналоговых сигналов. Устройство оцифровывания аналоговых каналов называется **кодеком**. Дискретные способы модуляции основаны на дискретизации непрерывных процессов, как по амплитуде, так и во времени (рис. 3.8). Рассмотрим принцип дискретной модуляции на примере импульсно-кодовой модуляции **ИКМ**. Аналого-цифровое преобразование является первым этапом цифровой обработки сигналов. Как показывает само название, *аналого-цифровой преобразователь* (**АЦП**) является связующим элементом между аналоговым и цифровым участками тракта, преобразующим непрерывный аналоговый сигнал с выхода микрофона в цифровую форму. Соответственно, *цифро-аналоговый преобразователь* (**ЦАП**) – последний элемент в цифровом тракте и задача его прямо противоположная: он преобразует цифровой сигнал в аналоговый, а последний поступает на динамик, преобразующий его в акустический сигнал, воспринимаемый ухом.

Работа АЦП складывается из двух этапов: замер амплитуды входного непрерывного сигнала во времени через равные интервалы времени, а затем представление каждого замера в виде двоичного числа определенной разрядности. Этот процесс схематически иллюстрируется на рис. 8, на котором моменты дискретизации показаны штрихами на оси времени и для трех моментов дискретизации указаны уровни сигнала – в десятичном (235, 220 и 191) и соответственно в двоичном представлении (11101011, 11011100 и 10111111).

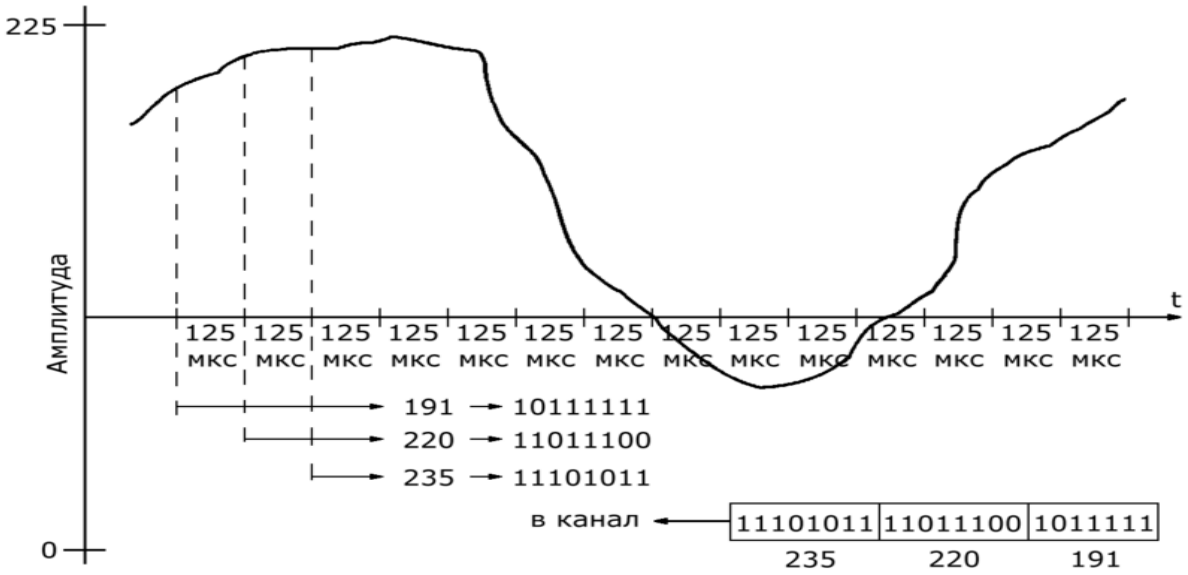


Рис. 3.8. Принцип работы аналого-цифрового преобразователя

В соответствии с теоремой Найквиста-Котельникова для качественной передачи голоса достаточно выбрать частоту дискретизации, в два раза превышающую наибольшую частоту в спектре обрабатываемого сигнала. Поскольку при передаче сигналов речи по телефонным каналам связи используется полоса частот от 300 до 3400 Гц, частота дискретизации выбрана 8000 Гц, т.е. с некоторым запасом.

В методе ИКМ обычно используются 7 или 8 бит кода для представления амплитуды одного замера. Для ИКМ скорость передачи по каналу соответственно равна 8000x8=64Кбит/с и 8000x7=56Кбит/с.

3.6. Цифровое кодирование и синхронизация

Цифровая передача сигналов основана на использовании дискретных состояний канала для передачи по нему информации.

Для того чтобы приемник точно знал в какой момент времени необходимо считывать бит информации с линии связи служит поимпульсная синхронизация. Любой резкий перепад переднего или заднего фронта бита используется для поимпульсной синхронизации. Лучшей синхронизационной комбинацией является чередование единиц и нулей.

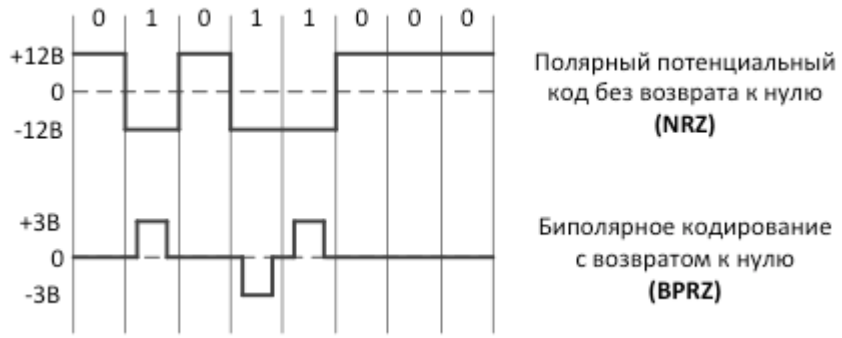


Рис. 3.9. Примеры схем кодирования

Проблема в синхронизации возникает тогда, когда необходимо передать длинную последовательность из нулей или единиц. Как видно из рис. 3.9, это относится к схеме полярного кодирования.

В стандарте одной из цифровых систем определено, что по каналу не должно передаваться более 15 последовательно идущих единиц или нулей, иначе вероятно, что синхронизация будет потеряна.

Для решения этой задачи синхронизации при цифровом кодировании используются два метода. Первый основан на добавлении в исходный код избыточного бита, содержащего логические единицы. Однако при этом снижается пропускная способность канала. Другой метод основан на предварительном перемешивании исходной информации таким образом, чтобы предотвратить появление длинной последовательности нулей или единиц. Такая операция называется скремблированием. При скремблировании используется известный алгоритм, поэтому преемник восстанавливает с помощью дескремблера исходную последовательность. Избыточные биты при этом в канал не передаются.

Разработано множество схем представления цифровых сигналов, или, иначе, цифрового кодирования, две из которых приведены на рис. 3.9. В верхней части рисунка показана биполярная схема кодирования сигналов, в которой цифровая 1 представлена напряжением -12В, а цифровая 0 – напряжением +12В. В нижней части рисунка показана биполярная схема с возвратом к нулю, в которой цифровые нули представлены отсутствием напряжения, а цифровые единицы – знакочередующимися трёхвольтовыми импульсами.

3.7. Частотное и временное мультиплексирование

Концепция мультиплексирования на физическом уровне показана на рис. 3.10.

Рис. 3.10. Концепция мультиплексирования на физическом уровне

Мультиплексор изображается как треугольник и объединяет множество низкоскоростных каналов в один высокоскоростной канал. Главное достоинство мультиплексирования (уплотнения) заключается в сокращении количества физических устройств и связанных с ними затрат. Впервые мультиплексирование было применено в телефонных сетях, что позволило создавать одновременно большое количество соединений между пользователями, используя незначительное количество физических устройств. Мультиплексирование может быть выполнено с аналоговыми каналами или с цифровыми. В первом случае используется техника частотного мультиплексирования, во втором – мультиплексирования с разделением времени.

3.7.1. Частотное мультиплексирование

Частотное мультиплексирование **FDM** (Frequency Division Multiplexing) показано на рис. 3.11. В FDM широкополосный аналоговый канал делится на несколько отдельных каналов. На рисунке широкополосный канал с полосой пропускания 40 кГц делится на 10 подканалов каждый по 4 кГц.

Канал 1	0 - 3999 Гц
Канал 2	4000 - 7999 Гц
Канал 3	8000 - 11999 Гц
Канал 4	12000 - 15999 Гц
Канал 5	16000 - 19999 Гц
Канал 6	20000 - 23999 Гц
Канал 7	24000 - 27999 Гц
Канал 8	28000 - 31999 Гц
Канал 9	32000 - 35999 Гц
Канал 10	36000 - 39999 Гц

Рис. 3.11. Частотное мультиплексирование (FDM)

Так как отдельно взятый разговор по телефону использует приблизительно 4 кГц от полосы пропускания, такой мультиплексор может передавать 10 телефонных разговоров через тот же самый физический канал, который раньше мог использоваться только для одного соединения. Технология, при помощи которой реализуется FDM, называется модуляцией несущей (carrier modulation). Каждый из поддерживаемых мультиплексором каналов оперирует несущей частотой, расположенной в полосе частот, отведенной для подканала. У передатчика узкополосный сигнал должен быть мультиплексирован в выделенный подканал, модулируемый несущей частотой, а затем размещен в определенном месте в системе. У приемника подканал выделяется и затем демодулируется, чтобы удалить несущую частоту. То, что остается, является первоначальным узкополосным сигналом, который был модулирован при передаче.

Частотное мультиплексирование является технологией, при помощи которой многие радиостанции совместно используют выделенную область частотного спектра. Результатом является демодулированный сигнал, который может быть воспринят человеческим ухом. В настоящее время технология FDM широко используется различными системами связи, включая системы мобильной телефонной связи.

3.7.2. Методы построения аппаратуры частотного мультиплексирования

В России на первичной сети связи сегодня применяется аппаратура частотного уплотнения (К-60 и К-1020с на симметричном кабеле и К-120, К-300, К-1920, К-3600 на коаксиальном кабеле).

На рис. 3.12 приведена схема, показывающая принцип построения аппаратуры с частотным разделением каналов.

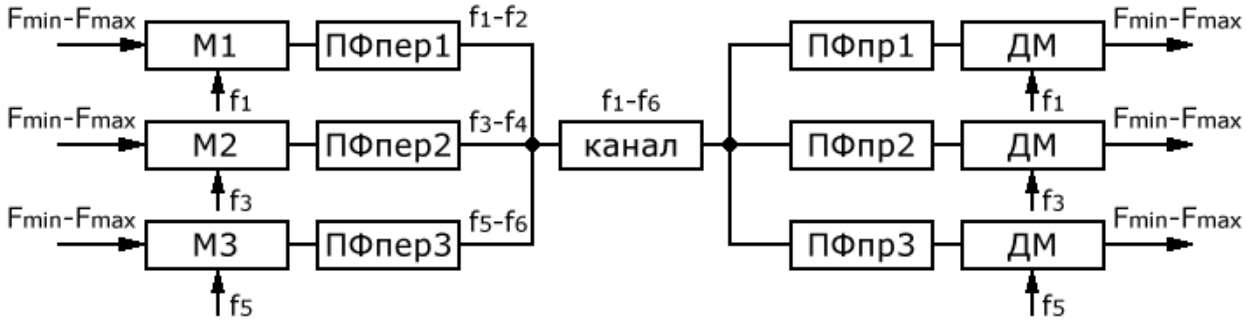


Рис. 3.12. Принцип построения аппаратуры с частотным уплотнением

Приведённая схема позволяет одновременно передавать по линии сообщения трёх соединений. Передающее устройство содержит три комплекта *модуляторов* (М1, М2, М3), которые осуществляют преобразование трёх одинаковых спектров исходных сигналов с частотами Fmin – Fmax в три различные по спектру полосы частот (f1-f2, f3-f4, f5-f6), проходя предварительно через полосовые фильтры ПФпер. Все сигналы в спектре частот f1-f6 поступают в канал. В приёмном устройстве имеются три комплекта полосовых фильтров ПФпр, имеющие такие же полосы пропускания, как и соответствующие полосовые фильтры в передающем устройстве. Эти фильтры служат разделительным устройством, так как пропускают на каждый *демодулятор* **ДМ** приёмного устройства только те частоты, пришедшие с линии, для которых этот демодулятор предназначен. Каждый демодулятор преобразует спектр пришедших по линии сигналов в исходный спектр Fmin-Fmax.

3.7.3. Временное мультиплексирование

Спектральная энергия сигнала при цифровой передаче не может быть размещена в частотной области. Прямоугольник может быть представлен как совокупность базовой синусоидальной волны и бесконечного числа “гармоник”, которые формируются согласно некоторой математической зависимости. Каждая гармоника имеет более высокую частоту и меньшую амплитуду, чем базовая синусоидальная волна. Таким образом, прямоугольные сигналы содержат составляющие бесконечно высокой частоты. Когда для улучшения качества речи телефонные линии стали использовать технологии цифровой передачи сигналов, понадобилось разработать новый способ мультиплексирования, т.к. частотное

мультиплексирование попросту невозможно реализовать с цифровыми сигналами при аналоговой передаче.

Мультиплексирование с разделением времени **TDM** (или временное мультиплексирование) (Time Division Multiplexing) проиллюстрировано на рис. 3.13.

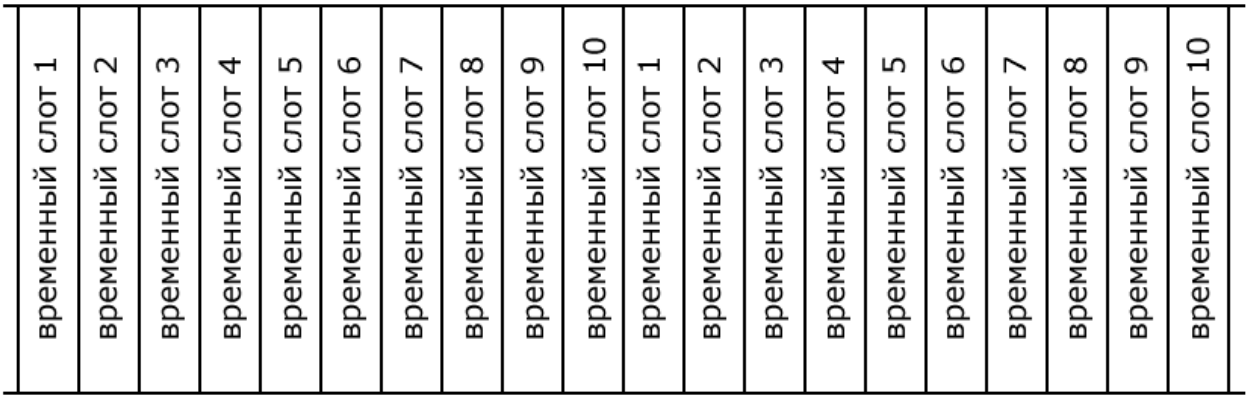


Рис. 3.13. Мультиплексирование с разделением времени (TDM)

Высокоскоростной канал связи делится на множество отдельных временных слотов и каждому низкоскоростному каналу выделяется определенный временной слот. Когда выделенный каналу временной слот становится доступен, то пока длится этот слот, для низкоскоростной передачи данных используется вся пропускная способность высокоскоростного канала связи. Следующий слот задействуется другой низкоскоростной передачей и т.д. Мультиплексирование с разделением времени широко используется в системах передач сигналов. В качестве примера можно привести наземные телефонные сети, где TDM встречается как в технологиях организации абонентского доступа, так и в технологиях организации межстанционных линий связи.

Две технологии мультиплексирования – FDM и TDM – могут быть объединены. То есть подканал в системе с частотным мультиплексированием может быть разбит дальше на несколько каналов, используя мультиплексирование с разделением времени. Подобным образом работают сотовые сети связи стандарта GSM.

Начало технологии мультиплексирования с разделением времени было положено разработкой мультиплексора **E1** (европейского варианта) и **T1** (американского варианта). Мультиплексор E1 позволяет в цифровом виде уплотнять голосовой трафик 30 абонентов, а T1 – 24 абонентов. На рис. 3.14 приведен 125 микросекундный цикл передачи в системе ИКМ-30, состоящий из 30 слотов информационных каналов передачи (составляющий один

кадр), одного служебного канала и одного канала синхронизации. Каждый канал занимает слот, в котором размещается один байт.

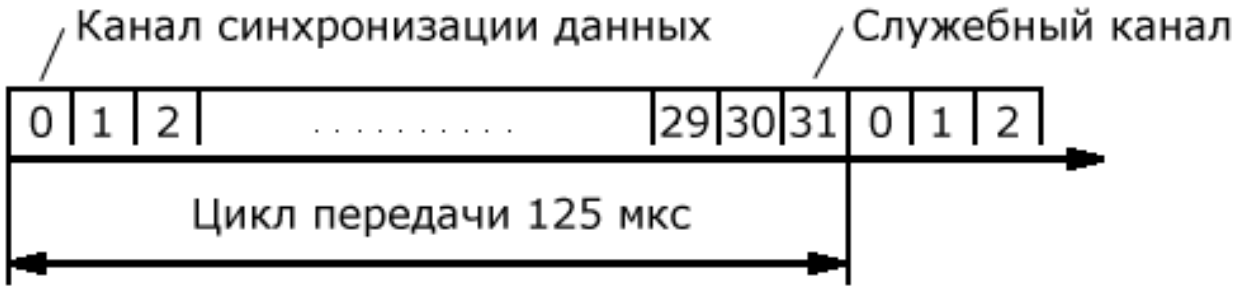


Рис. 3.14. Цикл передачи E1 (в системе ИКМ-30)

Информационный канал со скоростью передачи 64 кбит/с называется основным цифровым каналом ОЦК и обозначается Е0. Канал синхронизации (0) включает определенную комбинацию бит (0011011) и служит для определения начала цикла. Служебный канал служит для установления связи (по нему передаются импульсы от номеронабирателя, сообщение занятости абонента и др.).

В ИКМ-30 слот канала занимает 1 байт. Общая скорость передачи кадра E1 составляет 32 * 64 кбит/с=2 048 кбит/с.

При построении цифровых систем передачи введено понятие иерархических уровней, полагая, что на первом из них используются мультиплексоры E1 и T1. Мультиплексоры первого уровня типа n:1, по определению формируют из n входных цифровых каналов передачи один выходной. В случае мультиплексора E1 n=30, а T1 – n=24. Мультиплексоры второго уровня типа m:1 объединяет выходы мультиплексоров первого уровня; мультиплексоры третьего уровня типа p:1 объединяют выходы мультиплексоров третьего уровня и т.д. Это называют каскадным соединением мультиплексоров. На каждом уровне иерархии мультиплексор на выходе имеет свою скорость передачи (на втором – n*m, на третьем – n*m*p и т.д.). Варьируя коэффициенты кратности n, m, p, можно сформировать различные иерархические наборы скоростей передачи и цифровые иерархии цифровой системы передачи, которым соответствуют определенное количество ОЦК на выходе мультиплексора соответствующего уровня.

В России сегодня на первичной сети связи применяется аппаратура временного уплотнения ИКМ-30, ИКМ-120, ИКМ-480 на симметричных кабелях и ИКМ-480, ИКМ-1920 на коаксиальных кабелях. Цифры указывают на число каналов основных цифровых каналов

ОЦК, на которые рассчитаны эти системы передачи.

В таблице 3.1 приведены принятые в Европе иерархические уровни цифровых скоростей.

Таблица 3.1. Иерархические уровни цифровых скоростей (в Европе).

Уровень иерархии	Количество каналов ОЦК	Количество каналов предыдущего уровня (коэ□фициент□мультипл□ ксирования	Скорость Кбит/с
E0	1	1	64
E1	30	30	2048
E2	120	4	8488
E3	480	4	34368
E4	1920	4	139264

Аналогом систем Е-каналов в стандарте Американского национального института стандартов (**ANSI**) являются каналы типа Т1, Т2 и Т3 с отличающимися скоростями - 1,544Мбит/с, 6,312Мбит/с, 44,736Мбит/с. Для создания указанных в таблице уровней используется технология плезиохронной цифровой иерархии **PDH** (Plesiochronous Digital Hierarchy). Приведенные в таблице уровни иерархии позволяют передавать по каналам речь, факсы, телевизионное изображение.

Глава 4. Информационные процессы на канальном уровне сети X.25

4.1. Временная диаграмма последовательности обмена кадрами

Настоящая глава посвящена описанию основной процедуры второго (канального) уровня сети X.25 (X.25/2) – обеспечению безошибочного обмена информационными кадрами, передаваемых по подверженным помехам каналам связи [11,12]. Эта функция называется управление потоками и используется не только для сети пакетной коммутации стандарта X.25, но и для других сетей, обеспечивающих службу передачи данных. При этом алгоритм реализации этой функции отличается в сетях разных технологий. Для сетей связи, обеспечивающих службу телефонии или видео, управление потоком не производится. Основной принцип управления потоками в X.25/2 состоит в следующем. Передаваемый информационный кадр сохраняется в памяти передающего узла, ожидая приема квитанции о правильном приеме кадра узлом-получателем. В качестве этих узлов могут быть смежные транзитные коммутаторы или оконечный коммутатор. В следующей главе приводится описание структурных схем программного обеспечения по реализации функции управления потоками в X.25/2. Поэтому в настоящей главе приводится относительно подробное описание этой функции. Под кадром понимается элемент данных протокола PDU X.25/2 (между оконечным пунктом и ЦКП или между смежными ЦКП). Помехи в канале связи могут вызывать потерю, дублирование, искажение кадра, нарушение порядка прибытия кадра адресату. Кадр состоит из последовательности байтов. В начале и в конце кадра устанавливается синхронизирующий байт для определения начала и конца кадра. Этот синхронизирующий байт («01111110») называется флагом, а процедура обеспечения синхронизации бит-стаффингом. Для того чтобы можно было передавать байт такого содержания в информационной части кадра перед передачей после пяти непрерывных информационных «1» производится вставка «0» и изъятие этого бита на приеме.

Выполнение функции безошибочного обмена информационными кадрами обеспечивается подмножеством высокоуровневого протокола управления каналом **HDLC** (High-level Data Link Control) - процедурой сбалансированного доступа **LAP-B** (Link Access Protocol-Balanced). Этот протокол обеспечивает режим работы, в котором оба взаимодействующих в соединении узла равноправны.

Для описания алгоритма работы канального уровня сети X.25 используются **примитивы.** Примитивами являются блоки данных определенного вида, которые передаются между

уровнями системы для вызова различных процедур. Примитивы определяются согласно рекомендации ITU-T X.210. На рис. 4.1 представлен обмен примитивами между уровнями модели OSI. Показаны четыре типа примитивов – запрос, индикация, ответ, подтверждение.

Рис. 4.1. Обмен примитивами между уровнями модели OSI

В некоторых случаях достаточно двух типов примитивов (запрос, подтверждение).

На рис. 4.2 приведена временная диаграмма последовательности обмена кадрами при установлении соединения, передача одного информационного кадра и разъединение соединения. Приведем эту последовательность.

Рис. 4.2. Временная диаграмма последовательности обмена кадрами при установлении соединения, передаче информационного кадра и разъединении канального соединения

С сетевого уровня на канальный уровень станции А передаётся примитив «Запрос соединения». При выполнении этого примитива в канал связи с канального уровня передаётся кадр SABM о запросе соединения. При поступлении этого кадра на станцию Б он передаётся канальным уровнем на сетевой уровень в виде примитива «Индикация запроса соединения», в ответ на который выдается примитив «Ответ на запрос соединения». В результате в канал с канального уровня отправляется кадр UA о согласии на соединение. После приёма этого кадра с канального уровня на сетевой уровень станции Б направляется примитив «Подтверждение соединения». С сетевого уровня на канальный уровень станции А передаётся примитив «Запрос на посылку пакета данных». При выполнении этого примитива в канал связи с канального уровня передаётся информационный кадр «I» на противоположную станцию. Кадр «I», поступивший со станции А, передаёт сетевому уровню пакет данных с помощью примитива «Индикация прибытия правильного пакета данных». С канального уровня станции Б в канал передаётся кадр «RR» подтверждения приёма правильного пакета данных. Как видно из рис.4.2, далее показан обмен примитивами и кадрами (DISC и UA) фазы завершения работы соединения.

4.2. Формат кадра

На рис. 4.3 приведен формат информационного кадра X.25. Этот формат включает заголовок кадра З2, концевик кадра К2 и пакет данных третьего уровня. Кадр обрамляется *флагами* (**F**). Основным полем заголовка З2 является поле управления потоком, в котором основными характеристиками являются тип кадра и номера передаваемого и принимаемого информационного кадра: соответственно – N(S) и N(R).

Рис. 4.3. Формат информационного кадра X.25

Управление потоком в канале (например, между смежными узлами в сети X.25) состоит в следующем. Передаваемый кадр сохраняется в буфере передающего узла, ожидая приёма квитанции о правильном приёме кадра узла получателя. Если кадр был искажен в канале, то передача должна быть повторена.

Поле «Данные» (пакет сетевого уровня «Д») присутствует только в информационном кадре («I»). З3 означает заголовок пакета «Д». Концевик включает в себя контрольно-проверочную

комбинацию КПК (К2), необходимую для выявления кадров, искаженных помехами в канале. Кроме информационных кадров в процедуре используются супервизорные кадры RR, REJ для подтверждения или запроса повторной передачи «I» кадров, принятых с искажениями из-за помех в канале, а также кадр RNR для приостановки передачи информационных кадров при перегрузке принимающей стороны. Эти кадры включают только параметр N(R). Ненумерованные кадры (SABM, DISK, UA и др.) служат, например, для установления или разъединения соединений между смежными узлами коммутации.

Убедимся в необходимости применения при службе передачи данных схем обнаружения ошибок в принимаемых кадрах. Для этого определим вероятность появления таких искаженных кадров. Обозначим вероятность единичного ошибочного бита через P_B – эта характеристика канала, именуемая также *частотой ошибочных битов* (bit error rate – BER). При использовании каналов в сети X.25 эта величина может составлять P_B=0,0001. Если считать, что в канале возникают одиночные ошибки, статически независимые, то при длине кадра X.25 порядка L=128 байт вероятность безошибочного приема кадра

$P=(1-P_B)=(0,9999)^{1024} = 0,9$, т.е. каждый десятый кадр искажен на приеме.

Частота появления ошибочных бит в аналоговом канале сети X.25 нередко составляет даже P_B = 0,001. Ошибки в каналах связи чаще бывают не единичными, а групповыми, то есть имеет место пакетирование ошибок. Это значительно уменьшает частоту искаженных кадров.

Полученный результат свидетельствует о необходимости применения схем обнаружения ошибок. Работа всех методов обнаружения ошибок основывается на использовании помехоустойчивого кодирования. На передающей стороне заголовок 32 и информационная часть, которая присутствует только в информационных кадрах, представляется как последовательность из k бит, которую требуется защитить от ошибок. К данной последовательности добавляется контрольно-проверочная комбинация КПК (она имеет еще название контрольная последовательность кадра, FCS – frame check sequence), которая вычисляется по определенному алгоритму как функция k битов передаваемого кадра. В результате формируется кодовая комбинация, имеющая длину n бит и включающая контрольно-проверочную комбинацию (n-k) бит (рис. 4.4). На приеме из кадра выделяется КПК. На основании принятых k бит приемник вычисляет КПК и сверяет результат вычисления с принятой КПК. Если принятая и вычисленная КПК не совпадают, кадр считается искаженным и аннулируется. В сети X.25 используется один из наиболее широко используемых методов обнаружения ошибок – с помощью циклического избыточного кода **CRC** (Cyclic redundancy check). В сети X.25 n-k = 16 бит.

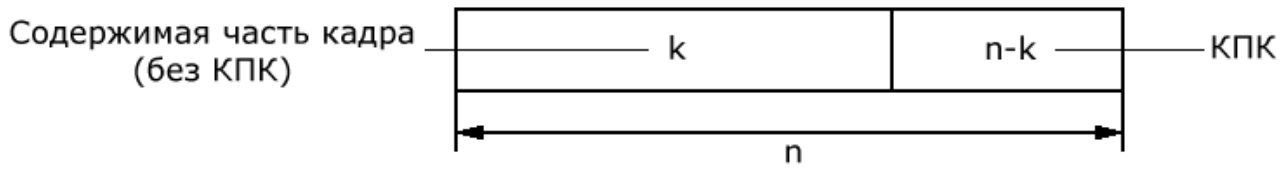


Рис. 4.4. Контрольно-проверочная комбинация в составе кадра из n бит

В разделе 4.4 приводится описание кода CRC тремя способами: с помощью арифметики по модулю 2, с использованием полинома, аппаратная реализация. Циклический код используется не только в сетях X.25, но и в IP - сетях, в беспроводных сетях стандарта GSM и др.

4.3. Восстановление информационных кадров

Приведем описание алгоритма передачи последовательности кадров X.25 в условиях помех в каналах связи. Такой алгоритм называется *управлением потоками на канальном уровне*. Все передаваемые «I» кадры заносятся в буфер передатчика и ожидают получения положительного подтверждения от противоположной принимающей стороны. По запросу противоположной стороны производится повторная выдача из буфера принятых с искажениями «I» кадров. В измененном алгоритме восстановление блоков данных из-за помех в каналах связи применяется и в других технологиях сетей связи как, например, на транспортном уровне IP-сети, в сети ТфОП и др. Достаточно подробное изложение алгоритма управления потоками в X.25 приводится для описания в следующей главе принципов составления алгоритмов программного обеспечения.

На канальном уровне X.25 восстановление искаженных кадров предусматривает нумерацию передаваемых «I» кадров. Для описания метода в рекомендации ITU-T X.25 введены следующие обозначения:

V(S) – переменная состояния передачи.

N(S) – порядковый номер передаваемого кадра «I». N(S) устанавливается равным V(S).

V(R) – переменная состояния приема.

N(R) - порядковый номер I-кадра, ожидаемого на прием.

V(S) означает текущий порядковый номер кадра «I», содержащего пакет данных и подлежащего передаче на физический уровень. Переменная V(S) в нормальном режиме функционирования звена данных принимает значения по модулю 8 (в цикле от 0 до 7), в

расширенном режиме - по модулю 128 (в цикле от 0 до 127). Расширенная нумерация применяется в каналах с большим временем задержки (межконтинентальная связь или спутниковые каналы). По окончании передачи кадра значение V(S) увеличивается на единицу.

Переменная V(R) содержит текущее значение порядкового номера очередного кадра «I», который ожидают на приеме. Для V(R), как и для V(S), приняты нормальный и расширенный режимы нумерации. После приема I-кадра, в котором не обнаружены ошибки, и номер которого совпадает с ожидаемым приемной стороной N(S)=V(R), значение V(R) увеличивается на единицу.

N(R) – порядковый номер I-кадра, ожидаемого на прием. N(R) содержится в заголовке (32) принимаемых кадров «I» и в супервизорных кадрах RR, REJ, RNR. N(R) в кадрах RR и «I» указывает, что переданные с противоположной стороны канала кадры «I» с номерами N(S)<N(R) были приняты правильно.

Информационный кадр «I» содержит оба параметра N(S) и N(R). Информационные кадры стираются из буфера повторной передачи при подтверждении правильного приема.

Супервизорный кадр готовность к приему RR (receive ready) является положительной квитанцией, поступающей от принимающей стороны, и указывает на то, что переданные «I» кадры с номерами N(S)<N(R) приняты правильно и могут быть стерты из буфера повторной передачи. Здесь N(R) является параметром кадра RR. В случае приема «I» кадра входящий в него параметр N(R) также является положительной квитанцией кадров буфера с N(S)<N(R).

Супервизорный кадр отказ REJ (reject) является отрицательной квитанцией и указывает, что «I» кадры, с номерами N(S)<N(R) приняты правильно. А кадры с номерами, начиная с N(S)=N(R), должны быть повторно переданы из буфера. Повтор из буфера «I» кадров может потребоваться также по истечении определенного времени, в течение которого не была получена положительная квитанция RR о приеме. Предельное число «I» кадров, переданных и не получивших подтверждение RR, называется *шириной окна* W. В этом случае очередной пакет данных с сетевого уровня не инкапсулируется в кадр «I» для передачи в канал.

Если в приемник поступил «I» кадр, в котором не обнаружены ошибки и с ожидаемым номером N(R), то служебные поля канального уровня (З2 и К2) отбрасываются, и входящий в кадр пакет данных передается с канального на сетевой уровень. На рис. 4.5 приведена временная диаграмма обмена «I» кадрами между пунктами А и Б (случай приема «I» кадров без искажения, исходное состояние V(S)=V(R)=0, буферы повтора пустые).

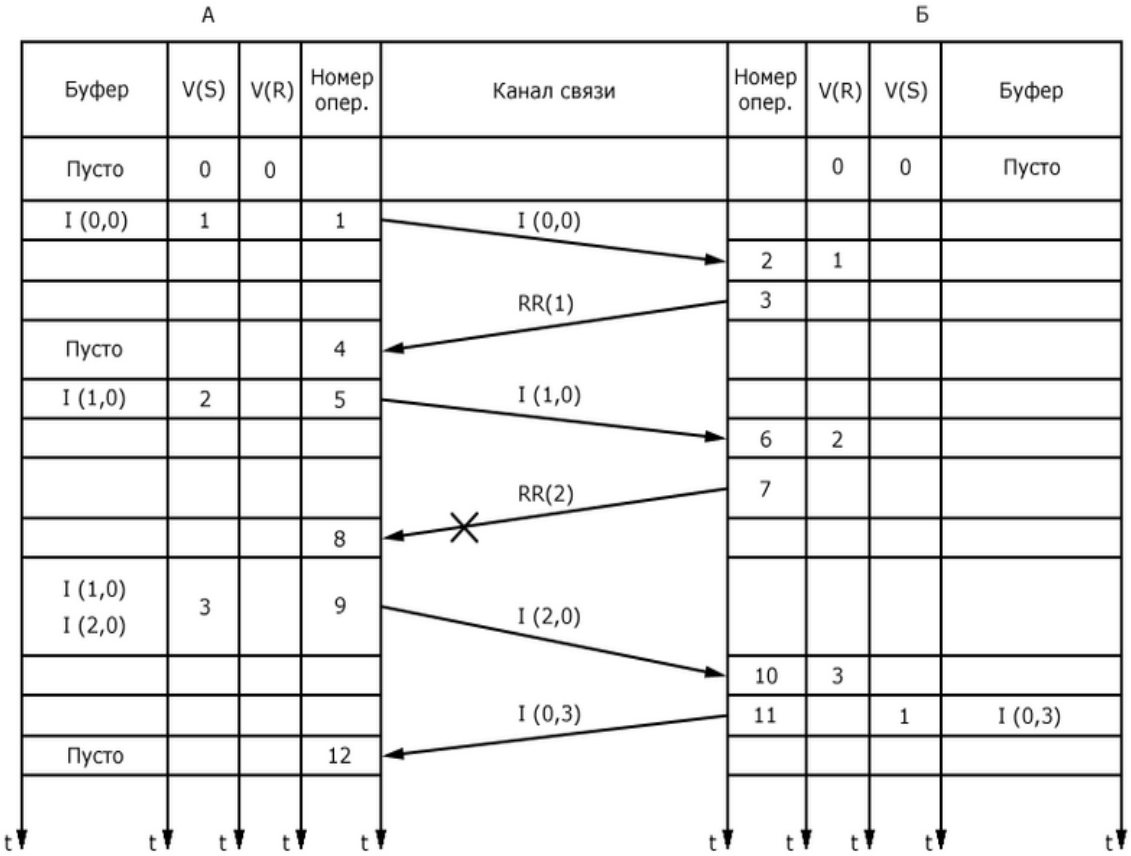


Рис. 4.5. Временная диаграмма обмена «I» кадрами, принятыми с канала без искажений

Обозначения:

- I (i, j) – информационный кадр с параметрами N(S)=i, N(R)=j
- RR(j) – кадр RR с параметром N(R)=j

Крестиком отмечен искаженный в канале кадр. Ниже приведено описание последовательности операций.

- Передача «I» кадра с параметрами N(S)=0, N(R)=0. Запись кадра «I» в буфер станции А. Изменение текущего значения V(S):=V(S) + 1, т.е. V(S)=1 (на станции А).
- Прием без ошибок I (0,0) на станции Б. Номер кадра N(S) совпадает с ожидаемым номером V(R), то есть N(S)=V(R)=0. Изменение текущего состояния приема V(R):=V(R)+1, т.е. V(R)=1 в Б.
- Подтверждение приема кадра I (0,0), т.е. передача положительной квитанции RR(1).
- Прием RR(1) и стирание из буфера кадра I (0,0).
- Передача кадра I (1,0), запись его в буфер, V(S)=2.
- Прием без ошибок I (1,0) на станции Б, V(R)=2.

- Подтверждение приема I (1,0), т.е. передача квитанции RR(2).
- Прием искаженного в канале кадра RR(2). Кадр отбрасывается.
- Передача очередного «I» кадра I (2,0), запись его в буфер (в буфере станции А теперь записаны два кадра I (1,0), I (2,0), которые ждут подтверждения об их приеме на станции Б), V(S)=3.
- Прием безошибочного I (2,0) на станции Б, V(R)=3.
- Передача «I» кадра со станции Б на станцию А с параметрами N(S)=0, N(R)=3, т.е. I (0,3). V(S)=1 (на станции Б), запись в буфер I (0,3) на станции Б. Этот кадр одновременно является квитанцией правильного приема станцией Б «I» кадров с номерами 1 и 2.
- Прием без ошибок I (0,3), стирание из буфера станции А кадров I (1,0) и I(2,0).

В приведенной на рис. 4.5 диаграмме все «I» кадры принимаются неискаженными. Поэтому операции приема этих кадров (2, 6, 10 на станции Б и 12 на станции А) завершаются передачей входящих в них пакетов данных на сетевой уровень.

На рис. 4.6 представлена диаграмма, включающая прием некоторых искаженных кадров «I». Для наглядности диаграммы параметры V(S) и V(R) на рисунке не приведены.

Как видно из диаграммы, искаженные в канале кадры I(2,0), I(3,0), I(4,0) при получении кадра REJ(1) передаются на станцию Б повторно из буфера. Кадры I(0,0) со станции А и I(0,4), I(1,5) со станции Б повторно из буферов не передаются, поскольку они подтверждаются соответственно кадрами RR(1), I(4,1) и RR(2). Необходимо отметить, что нумерация кадров N(S) и N(R) циклическая. При нормальной нумерации для этого отводится 3 бита, а при расширенной - 7 бит. Напомним, что под шириной (размером) окна W понимается максимальное число неподтвержденных кадров в буфере. При заполнении такого числа кадров в буфере согласно алгоритму требуется перейти к повторной передаче этих кадров из буфера. Чем выше пропускная способность канала и больше протяженность канала, тем размер окна выше.

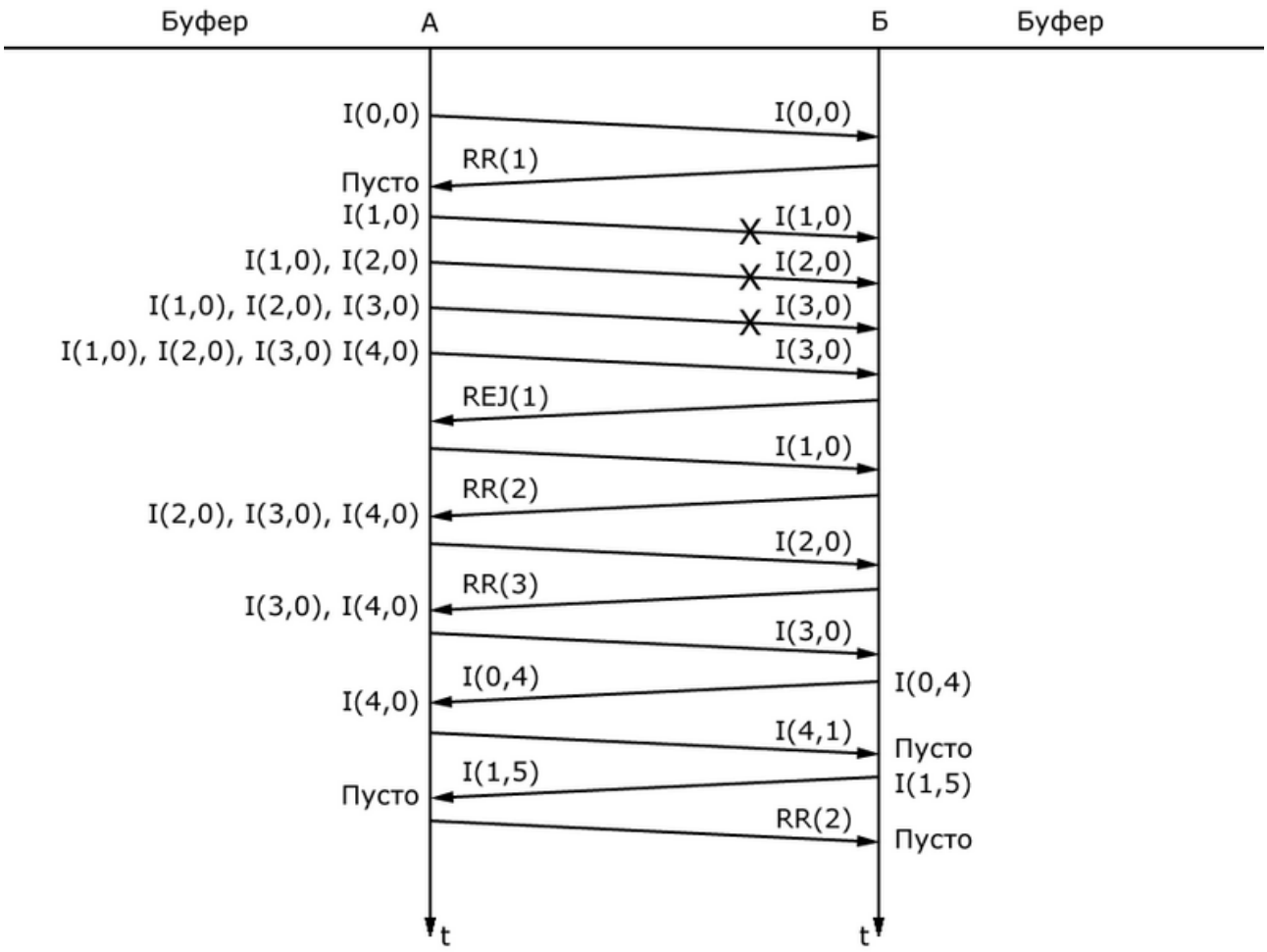


Рис. 4.6. Временная диаграмма восстановления «I» кадров при приеме отрицательной квитанции REJ

Рассчитаем величину задержки кадра длинной порядка 128 байт при скорости передачи 64 кбит/с. Задержка составляет 128 байт / 64 кбит/с = 16 мсек. Сравним эту величину со временем задержки распространения кадра по спутниковому каналу протяженностью 72000 км, приняв скорость распространения сигнала равной скорости света в вакууме – 300000 км/с. Эта величина составляет 72000 км / 300000 км/с = 240 мсек, т.е. в канале одновременно могут находиться 15 кадров (240/16). Отсюда ясно, почему при использовании спутниковых каналов в сети X.25 применяется расширенная нумерация и соответственно большая ширина окна W , чем при нормальной нумерации.

Порядковая нумерация не всегда гарантирует доставку отдельного кадра. В тех случаях, когда гарантированная доставка является важным фактором, также используются таймеры передатчика. Передатчик даёт приёмнику определённое количество времени на подтверждение успешной передачи. Если за выделенное время подтверждение от приёмника

не происходит, то передатчик повторно посылает кадр.

На рис. 4.7 и рис. 4.8 приведены диаграммы повтора «I» кадров из буфера по истечении тайм-аута. Примеры приведены для случая запрета передачи очередного кадра «I» при числе ожидающих в буфере повтора «I» кадров равном окну W (W=4).

Как видно из диаграммы, по истечении тайм-аута кадр «I» повторяется из буфера. Причиной повторения по таймеру может быть искажение только «I» кадров (рис. 4.7), либо искажение кадров «I» и кадров подтверждения RR (рис. 4.8). В случае правильного приема кадра I(0,0) пакет сетевого уровня должен быть отправлен на сетевой уровень, но повторный прием кадра I(0,0) считается копией уже принятого кадра, а поэтому он сбрасывается, т.е. не пересылается на сетевой уровень.

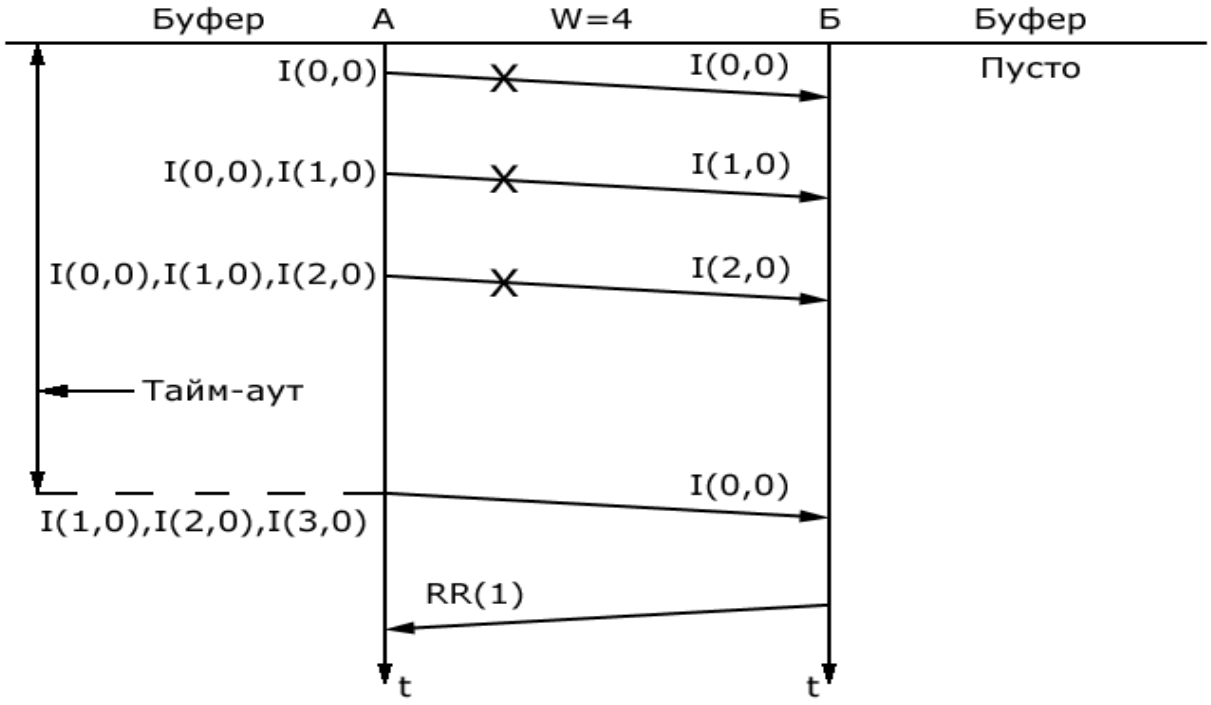


Рис. 4.7. Временная диаграмма восстановления кадра «I» по истечении тайм-аута

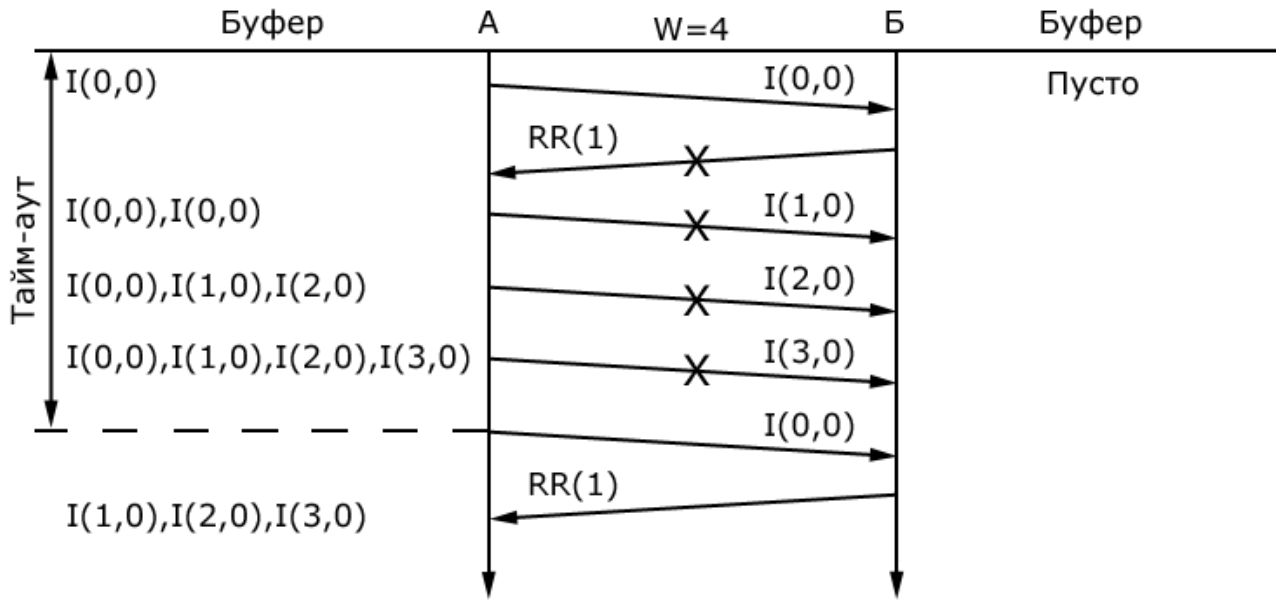


Рис. 4.8. Временная диаграмма сброса копии «I(0,0)» кадра, принятого повторно от станции Б, по истечении тайм-аута на станции А

4.4. Обнаружение ошибок с помощью избыточного циклического кода

Ниже приводятся три способа описания определения кода CRC: с использованием арифметики по модулю 2, с использованием полинома и аппаратная реализация [13].

4.4.1. Пример с использованием арифметики по модулю 2

В вычислениях по модулю 2 используется двоичное сложение без переноса в старший разряд (операция исключающего ИЛИ).

Введем следующие обозначения:

- *T* – n-битовый кадр, который необходимо передать;
- *D* – k-битовый блок сообщения (k первых бит кадра *T*);
- *R* – (n-k) – битовая контрольная последовательность кадра (последние (n-k) бит кадра *T*). Значение *R* необходимо вычислить;
- *P* - (n-k+1) – битовый делитель.

Пример:

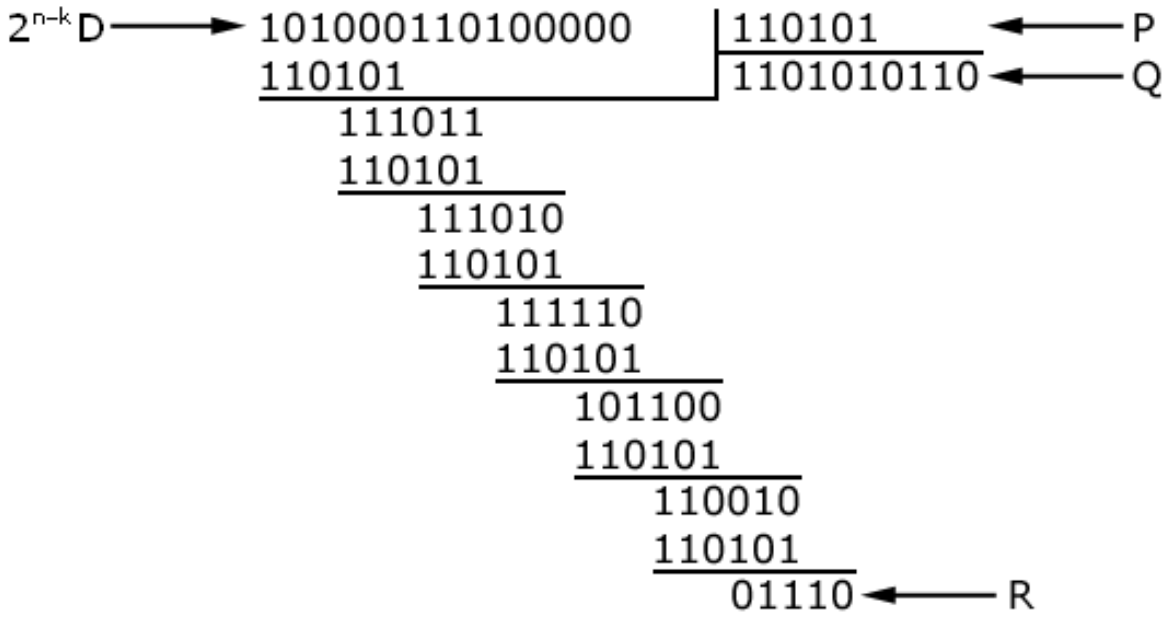
- Дано:

  сообщение *D* – 1010001101 (10 бит);

  последовательность *P* – 110101 (6 бит);

  Итак, n =15, k=10, n-k=5.

- Сообщение умножается на 2^{n-k}, что дает в результате: 101000110100000.

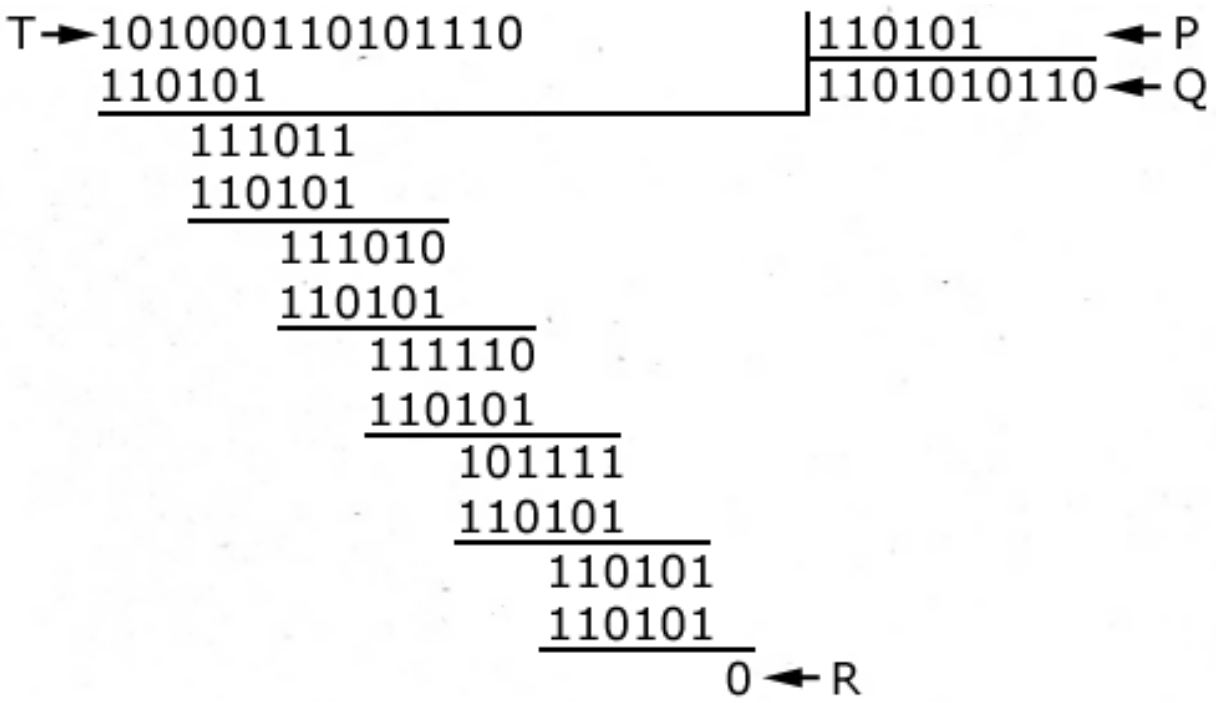


- Полученная последовательность делится на *P*:

  Здесь Q – целое число от деления.

- Полученный остаток складывается с $2^{n-k} * D$, результат (*T* = 101000110101110) передается.

- При отсутствии ошибок принятая последовательность *T* не отличается от переданной. Приемник выполняет деление на *P*:



Поскольку деление не дало остатка, считается, что ошибки отсутствуют.

4.4.2. Пример с использованием полинома

Используя предыдущий пример, получаем: последовательности D = 1010001101 соответствует полином $D(X) = X^9 + X^7 + X^3 + X^2 + 1$, последовательности P = 110101 - полином $P(X) = X^5 + X^4 + X^2 + 1$, последовательности R = 01110 − $R(X) = X^3 + X^2 + X$.

Полиномиальное деление, соответствующее приведенному ранее двоичному делению, показано на рис. 4.9.

Ошибка не обнаружится только в том случае, если соответствующий полином $E(X)$ делится на $P(X)$. При надлежащем выборе полинома $P(X)$ выявляются такие ошибки:

- все 1-битовые ошибки, если $P(X)$ имеет более одного ненулевого члена;
- все 2-битовые ошибки, если $P(X)$ имеет делитель из трех членов;
- любое нечетное количество ошибок, если в разложении $P(X)$ по множителям: присутствует $(X + 1)$;
- любой пакет ошибок, длина которого не превышает n-k, или, эквивалентно, не превышает длину контрольной последовательности кадра.

Здесь Q(X) – полином от Q.

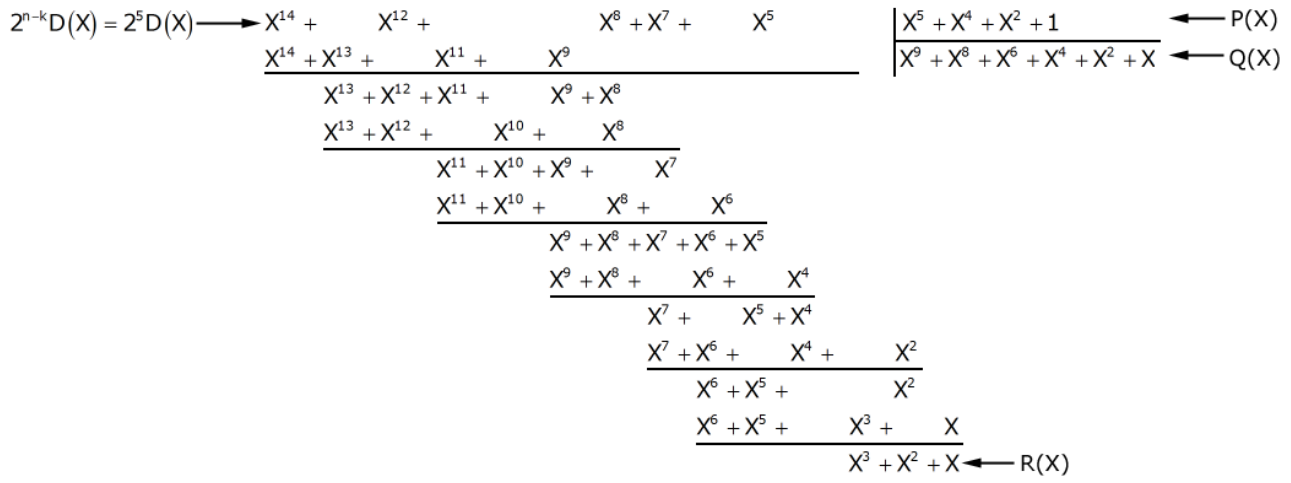


Рис. 4.9. Пример полиномиального деления

Приведем примеры длин n-k КПК (FCS) используемых полиномов P(X) в сетях связи:
CRC –3: в GSM.
CRC – 16: в ОКС№7, X.25, Интернет (на межсетевом уровне, на транспортном уровне по протоколу TCP).
CRC – 32: в ATM.

4.4.3. Пример аппаратной реализации

Процесс циклической проверки четности с избыточностью можно представить как схему деления, состоящую из элемента исключающего ИЛИ (сложение по модулю 2) и регистра сдвига. Регистр сдвига представляет собой строку 1-битовых ячеек памяти. Каждая ячейка имеет выходную шину, показывающую текущее хранимое значение, и входную шину. В дискретные моменты времени, которые называют тактами, значения ячеек памяти замещаются значениями, указанным во входной шине. Замена происходит синхронно во всем регистре, так что в результате значения ячеек регистра сдвигаются на один бит.

Реализация схемы выглядит следующим образом.

- Регистр, содержащий (n - k) бит (по размеру контрольно-проверочной комбинации).
- До (n - k) элементов исключающего ИЛИ.
- Наличие или отсутствие логического элемента соответствует наличию или

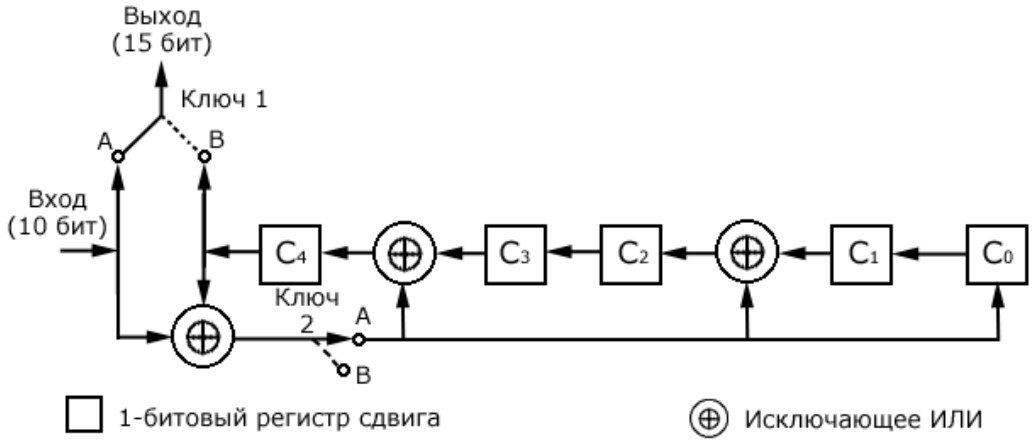
отсутствию члена в полиноме-делителе P (X), исключая члены 1 и X^{n-k}.

Понять архитектуру схемы деления можно с помощью примера, приведенного на рис. 4.10. В примере, как и выше, используются такие величины:

сообщение D = 1010001101; $D(X) = X^9 + X^7 + X^3 + X^2 + 1$;

делитель P = 110101; $P(X) = X^5 + X^4 + X^2 + 1$.

На рис. 4.10, а) представлена реализация регистра сдвига. Процесс начинается с очистки регистра (все ячейки обнуляются). После этого передаваемое сообщение (делимое) побитово вводится в регистр, начиная со старшего бита. На рис. 4.10, б) приведена таблица, которая иллюстрирует пошаговую работу схемы по мере введения отдельных битов. Строки таблицы содержат значения пяти ячеек регистра сдвига в соответствующие моменты времени. Кроме того, в строках таблицы приводятся значения на выходе трех схем исключающего ИЛИ. Последнее число в каждой строке - значение следующего входного бита, который станет доступен для работы на следующем этапе.



а) Реализация регистра сдвига

	C_4	C_3	C_2	C_1	C_0	$C_4 \oplus C_3 \oplus I$	$C_4 \oplus C_1 \oplus I$	$C_4 \oplus I$	I=Ввод
Исходное состояние	0	0	0	0	0	1	1	1	1
Этап 1	1	0	1	0	1	1	1	1	0
Этап 2	1	1	1	1	1	1	1	0	1
Этап 3	1	1	1	1	0	0	0	1	0
Этап 4	0	1	0	0	1	1	0	0	0
Этап 5	1	0	0	1	0	1	0	1	0
Этап 6	1	0	0	0	1	0	0	0	1
Этап 7	0	0	0	1	0	1	0	1	1
Этап 8	1	0	0	0	1	1	1	1	0
Этап 9	1	0	1	1	1	0	1	0	1
Этап 10	0	1	1	1	0				

Передаваемое сообщение

Рис. 4.10. Схема реализации аппаратным способом

Отметим, что операция исключающее ИЛИ влияет на значения ячеек С4, С2 и С0 при следующем сдвиге, что идентично рассмотренному ранее процессу двоичного деления. Процесс выполняется для всех битов передаваемого сообщения. Для обеспечения корректности выходного сигнала используются два ключа. При вводе битов данных оба ключа находятся в положении А. В результате за первые 10 шагов входные биты подаются в регистр сдвига и также используются в качестве выходных битов. По окончании обработки последнего бита данных регистр сдвига содержит остаток деления - содержание регистров после этапа 10. При вводе последнего бита данных в регистр оба ключа устанавливаются в положение В. В этом случае:

- все логические элементы больше не изменяют значения битов;
- за следующие 5 шагов на выход подаются 5 бит контрольно-проверочной комбинации

(т.е. содержимое регистров после этапа 10).

В приемнике используется аналогичная логика. Принятые биты последовательности М вводятся в регистр сдвига по мере поступления. Если ошибки отсутствуют, то после обработки М регистр сдвига будет содержать последовательность контрольно-проверочной комбинации КПК. После этого начинает поступать переданная последовательность КПК.

В результате на выход регистра будут подаваться двоичные нули и по завершении приема все ячейки будут иметь значение 0.

ГЛАВА 5. Структурные схемы программного обеспечения процедуры управления потоками сети X.25

Настоящая глава состоит из основной части, включающей структурные схемы программного обеспечения (ПО) процедуры управления потоками сети X.25, и дополнения, включающего алгоритмы для составления ПО в шести лабораторных работах.

5.1. Структурная схема организации ПО процедуры управления потоками сети X.25

Все программы второго уровня выполняются канальным процессором и подразделяются на фоновые программы, программу - диспетчер фоновых программ и программы обработки прерываний. На рис. 5.1 приведена упрощенная структурная схема организации этого программного обеспечения.

Рис. 5.1. Структурная схема организации программного обеспечения безошибочного обмена информационными кадрами на канальном уровне сети X.25

В следующих разделах приведены упрощенные структурные схемы фоновых программ, выполняющих функцию обеспечения правильной последовательности кадров [14]. Эти схемы могут быть использованы при разработке программ независимо от языка

программирования.

Фоновые программы в свою очередь на рисунке разделены на программы, обеспечивающие безошибочный обмен информационными кадрами ($П_{фо}$) и программы, выполняющие остальные функции канального уровня ($П_{фн}$). Все фоновые программы управляются диспетчером программ циклически и непрерывно.

Программы прерываний выделены в программы обработки одного или нескольких байтов на передачу в канал (на физический уровень) или на прием из канала (с физического уровня). Механизм прерываний осуществляет прерывание работы текущей фоновой программы, переводит к работе программы прерывания. По завершению работы программы прерывания возобновляется выполнение прерванной фоновой программы.

Фоновые программы, которые не выполняют функцию управления потоком, на рисунке изображены в виде одного квадрата. К ним относятся функции установления и разъединения соединения, функции взаимодействия с сетевым уровнем сети X.25 и другие функции.

Диспетчер программ (**ДП**) управляет последовательностью всех фоновых программ. Как видно из рисунка, все фоновые программы обеспечения правильной последовательности кадров разделены на программы передачи и программы приема.

Диспетчер программ запускает определенную фоновую программу, а после ее выполнения управление возвращается к диспетчеру с тем, чтобы он запустил другую фоновую программу.

Определение последовательности и частоты запуска программ является самостоятельной задачей оптимизации структуры программного обеспечения с точки зрения минимизации задержки обработки на приеме, потерь кадров и других качественных характеристик. Программы приема часто имеют приоритет перед программами передачи в службе передачи данных. В службе передачи речи или видео приоритет дается фоновым программам передачи. Это объясняется тем, что для обеспечения качества передачи данных важно не потерять пакет данных, а для качества передачи речи и видео важна величина задержки приема пакета при передаче.

Основной принцип работы большинства фоновых программ состоит в последовательной обработке блоков данных (кадров, пакетов и др.), находящихся в очередях на обслуживание программами. В случае конфигурации звена данных «точка-точка» образуются следующие очереди:

$О_{п32}$ – очередь пакетов на передачу с сетевого уровня на канальный уровень;

$О_{повт}$ – очередь «I» (информационных) кадров на случай необходимости повторной передачи кадров в канал;

$О_{кпм}$ – очередь всех принятых кадров с канала (т.е, физического уровня), в которых при анализе КПК (контрольно-проверочной комбинации) не было обнаружено ошибок;

$О_{п23}$ – очередь пакетов, подлежащих передаче с канального уровня на сетевой уровень.

Приведем упрощенные структурные схемы основных фоновых программ передачи ($Р1_{ПД}$, $Р2_{ПД}$, $Р3_{ПД}$, $Р4_{ПД}$, $Р5_{ПД}$, $Р6_{ПД}$, $Р7_{ПД}$), приема ($Р1_{ПМ}$, $Р2_{ПМ}$, $Р3_{ПМ}$, $Р4_{ПМ}$) с кратким описанием их функционирования. Напомним, что фоновые программы запускаются диспетчером программ ДП. По завершению работы фоновая программа возвращает управление ДП.

5.2. Структурные схемы фоновых программ

Ниже приводится описание работы фоновых программ, приведенных на рисунке 5.1 организации программного обеспечения. На этом рисунке указаны фоновые программы, описание структурных схем которых приводится в настоящем разделе.

Прежде, чем перейти к описанию указанных фоновых программ приведём диаграмму одного из примеров обмена кадрами между пунктами А и Б (рис. 5.2). Далее при описании работы фоновых программ по структурным схемам будем указывать какие фоновые программы выполняют соответствующую им функцию.

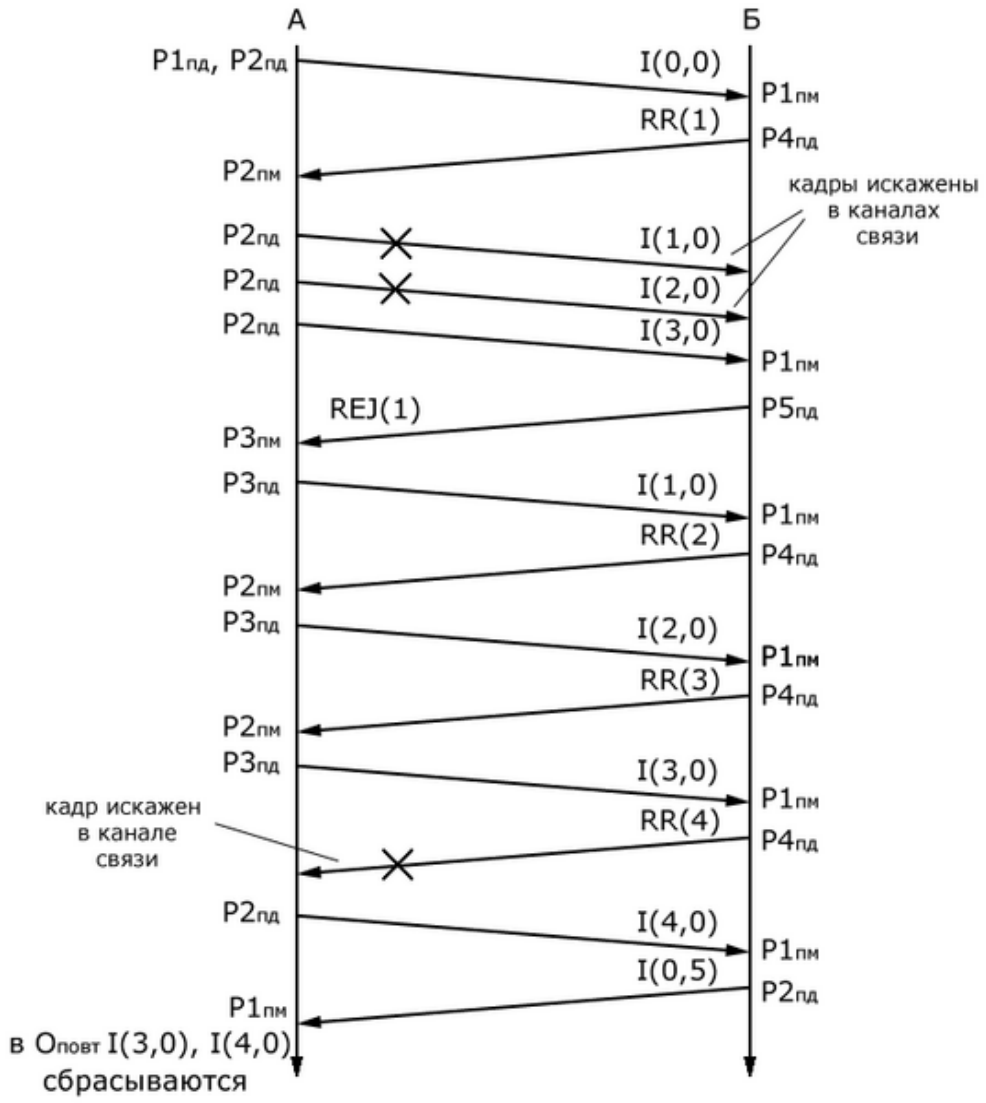


Рис. 5.2. Диаграмма обмена кадрами с указанием обработки фоновых программ

5.2.1. Основные положения составления ПО. Структурная схема $P1_{ПД}$ «Запрос и прием очередного пакета с 3 уровня»

На рис. 5.3 приведена структурная схема программы $P1_{ПД}$, ”Запрос и прием очередного пакета с 3 уровня” (т.е. с сетевого уровня). Приведенная схема ПО обеспечивает перенос пакета с сетевого уровня на канальный уровень **X.25**. Основные принципы составления ПО системы коммутации реального масштаба времени с большим числом команд.

Приведем основные положения, которых необходимо придерживаться при составлении ПО системы коммутации:

- иерархический принцип построения ПО (диспетчер программ, фоновые программы, подпрограммы);
- деление больших ветвей программ с целью упрощения отладки и модернизации ПО;
- выполнение большинства программ осуществляется путем обработки очередей сообщений, находящихся в различных областях оперативной памяти;
- составление программного обеспечения с наименьшим числом команд является одной из наиболее важных задач для обеспечения большего числа обслуживаемых пользователей коммутационной станцией и лучших показателей качества обслуживания.

Покажем работу приведенной на диаграмме рис. 5.2 программы $Р1_{ПД}$ (рис. 5.3).

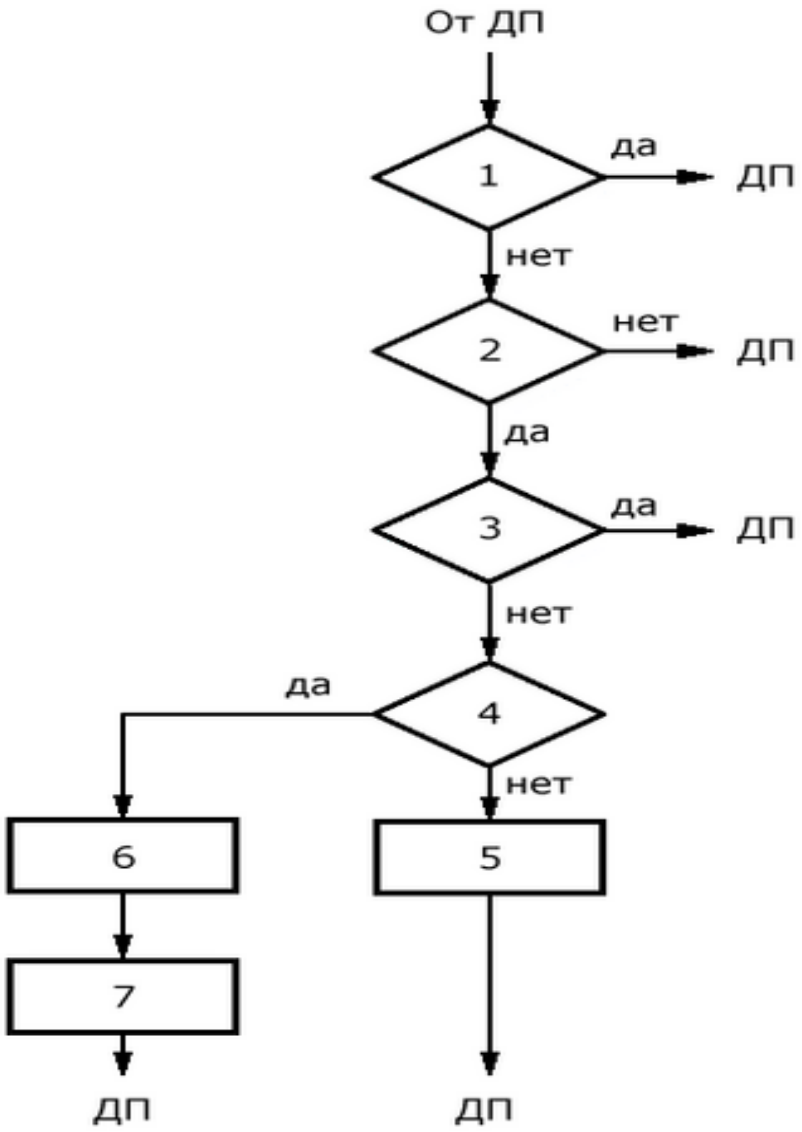


Рис. 5.3. Структурная схема $Р1_{ПД}$ ”Запрос и прием очередного пакета с 3 уровня”

Операция 1. Режим передачи очередного пакета в канал? Если да, то переход к диспетчеру программ ДП. Если нет, то переход к операции 2.

Операция 2. Проверка наличия пакета для передачи в канал. В случае такого признака производится переход к операции 3. Этот пакет находится на сетевом уровне.

Операция 3. Проверка числа кадров $N(O_{повт})$, находящихся в буфере повторной передачи. Если $N(O_{повт})$ равно *ширине окна* W, то возврат к ДП. Если нет, то переход к операции 4.

Операция 4. Эта операция иллюстрирует деление длинных программ на две. Вначале программа не находится в состоянии «запрос пакета с 3 уровня». Проверка состояния «запрос пакета с 3 уровня». В случае, если не находится в этом состоянии, то переход к операции 5. Иначе, переход к операции 6.

Операция 5. Установка состояния «запрос пакета с 3 уровня».

Операция 6. Поставить пакет 3 уровня в конец очереди $O_{п32}$ пакетов, подготовленных к передаче на канальный уровень.

Операция 7. Сброс состояния «запрос пакета с 3 уровня». Переход к ДП.

Как видно из схемы, диспетчер дважды обращается к программе $P1_{ПД}$ для того, чтобы осуществить прием одного пакета с третьего уровня: первый раз по цепочке операций 1 - 5, а второй раз 1 - 4, 6 - 7.

Все операции кроме операции 6 просто переводятся на язык программирования. Подробному описанию подлежит операция 6. Под блоком данных в сети X.25 будем понимать кадр (блок данных второго уровня) или пакет (блок данных третьего уровня). В других технологиях сетей блоки данных часто называются другими терминами (ячейка, фрейм и др.). Дадим определение массива блока данных, который стоит в очереди на обработку программой. Операция 6 производит установку пакета 3 уровня в очередь $O_{п32}$. Для построения такой очереди принятый пакет располагается в ОЗУ, где к информационным полям добавляются два служебных поля. Такой пакет со служебными полями будем называть массивом пакета. На рис. 5.4 представлен формат k-го массива пакета в очереди $O_{п32}$, где A_k - адрес начала k-го массива пакета. Первые два поля массива пакета являются адресными полями и занимают соответственно начальные адреса предыдущего и последующего массива

пакета.

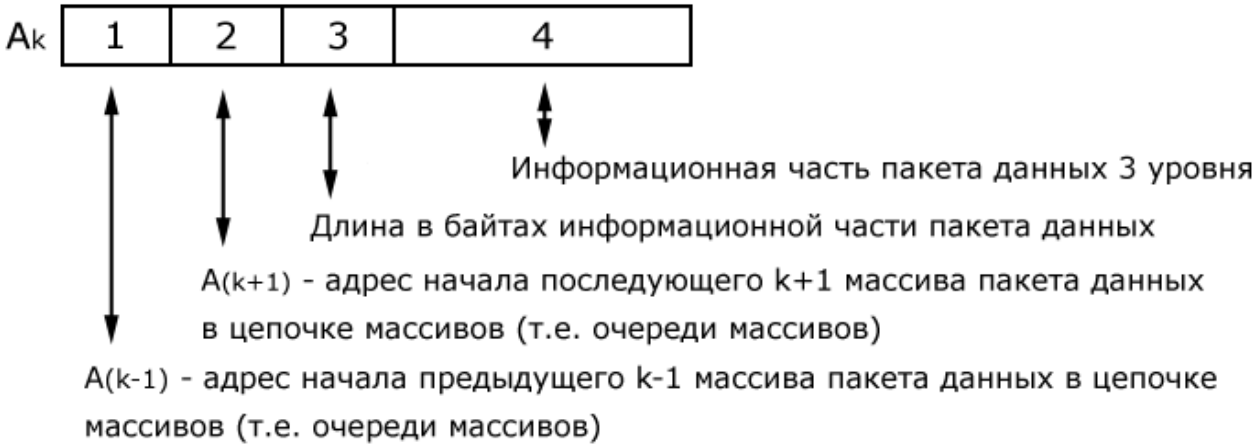


Рис. 5.4. Формат k-го массива пакета очереди $О_{п32}$

Массивы блоков данных (в данном случае массивы пакетов), образуют упорядоченную очередь, связывающую их друг с другом в процессе работы системы в реальном масштабе времени (хотя они располагаются в разных местах оперативной памяти). В качестве примера очереди $О_{п32}$ приведена очередь из трёх массивов пакетов с начальными адресами А1, А2, А3 (рис. 5.5.).

Рис. 5.5. Пример очереди из трех массивов пакетов

В поле 1 массива пакета 1 установлен 0, и в поле 2 массива последнего пакета 3 также установлен 0. В поле 2 массива пакета 1 указывается адрес начала массива пакета 2 (А2), а в

поле 2 массива пакета 2 - адрес начала массива пакета 3 (А3).

Третье поле (n1, n2, n3) означает длину данных соответственно пакета 1, пакета 2, пакета 3.

Алгоритм программного обеспечения часто выполняет следующую функцию: из очереди к одной фоновой программе снимается первый блок данных, и после его отработки устанавливается в хвост (конец) очереди другой фоновой программы. Для этой цели в каждой очереди блоков данных используется одномерная строка характеристики очереди, которая состоит из трёх полей (рис. 5.6). Для очереди $О_{п32}$ обозначим характеристику очереди $Н_{п32.}$ При составлении программного обеспечения оборудования сетей связи это дает возможность экономить машинное время, определив одной-двумя командами наличие или отсутствие блоков в очереди, адреса первого и последнего блока в очереди.

Рис. 5.6. Формат характеристики очереди

На рис. 5.7 приведена характеристика очереди для приведенного примера.

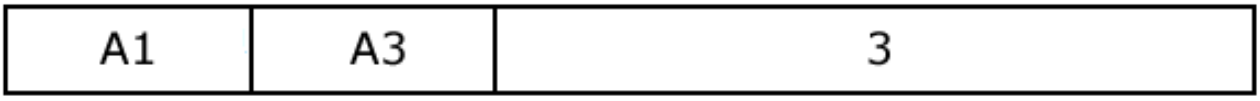


Рис. 5.7. Характеристика очереди

На этом примере покажем, каким образом реализуется операция 5 программы $Р1_{ПД}$ по установке пакета в конец очереди.

Допустим, начальный адрес массива этого пакета А4, в полях 3 и 4 установлены соответственно длина пакета в байтах и информационная часть пакета. В поле 2 массива

пакета устанавливается 0 (т. к. он занимает последнее место в очереди), в поле 1 устанавливается А3. В поле 2 массива пакета 3 с адресом А3 вместо 0 устанавливается значение начального адреса массива А4.

Приведём изменения в характеристике очереди. В поле 3 вместо 3 устанавливается новое число массивов пакетов в $О_{п32}$, т. е. 4, а в поле 2 вместо А3 устанавливается начальный адрес последнего массива пакетов в очереди, т.е. А4.

Работа фоновых программ часто заключается в обработке какого-либо массива очереди, снятии этого массива из одной очереди и установке его в другую очередь. Для организации таких очередей блоков данных с целью их обработки разными фоновыми программами создаётся очередь свободных блоков $О_{своб}$. Многие языки программирования высокого уровня предусматривают такую возможность. Первый в очереди $О_{своб}$ свободный блок используется для записи информационного блока (пакета, кадра и т.п.) и производится его установка в хвост (конец) очереди для обработки какой-либо фоновой программой. При освобождении блока данных после обработки фоновой программой этот блок заносится в хвост $О_{своб}$. Поле данных свободных блоков фиксировано, поэтому поле 3 (длина) отсутствует. В некоторых случаях могут быть несколько таких очередей $О_{своб}$ с разными длинами поля данных, что приводит к экономии оперативной памяти. Форматы массива очереди свободных блоков $О_{своб}$ и характеристика этой очереди $Н_{своб}$ во многом аналогичны описанному выше формату $О_{п32}$. Поле данных этих блоков свободно для записи конкретных блоков (например, для записи входных блоков данных с канала или с процессора другого уровня).

Передача информационных кадров в канал может осуществляться следующими тремя программами:

- передача очередного кадра «I», находящегося в очереди $О_{п32}$ (программа $Р2_{ПД}$);
- передача кадра «I» из очереди повтора $О_{повт}$ после получения отрицательной квитанции REJ с противоположного конца (программа $Р3_{ПД}$);
- передача кадра «I» из очереди повтора $О_{повт}$ после срабатывания таймера, указывающего на превышение допустимого времени ожидания подтверждения правильного приема кадра (программа $Р7_{ПД}$).

5.2.2. Структурная схема программы $P2_{ПД}$ - «Подготовка к передаче очередного «I» кадра в канал»

Покажем работу приведенной на диаграмме обмена кадрами (рис. 5.2) программы “Подготовка к передаче очередного «I» кадра в канал” (рис. 5.8).

Операция 1. Состояние «Передача кадра в канал»?

Длительность передачи (t) кадра в канал зависит от длины кадра L и пропускной способности канала V и равно

Например, при передаче в канал кадра «I» *L*=1000 бит и *V*=64 кбит/с время передачи кадра t=15,6 мс. Это означает, что при среднем времени выполнения одной команды 1 мкс во время передачи такого кадра в канал на все остальные фоновые программы предоставляется 15600 команд. Здесь *L*=1000 бит взята примерно равной длине пакета по умолчанию.

Операция 2. Есть пакеты в очереди $О_{п32}$. на передачу в канал? Если да, то переход к операции 3.

Значение числа пакетов в очереди $N(О_{п32})$ содержится в поле 3 характеристики очереди.

Операция 3. Снять первый пакет с очереди $О_{п32}$. и поставить в хвост очереди $О_{повт}$. Кадр этого пакета формирует операция 5.

Формат массива кадра $О_{повт}$ длиннее формата массива пакета $О_{п32}$, так как включает дополнительное поле – заголовок кадра. Для того чтобы не терять машинное время передачи содержимого поля данных из $О_{п32}$ в $О_{повт}$, целесообразно формат массива $О_{п32}$ сделать одинаковым с массивом данных $О_{повт}$, т.е. включить в него неиспользуемое поле заголовка кадра. Такая экономия машинного времени позволяет увеличить пропускную способность сети.

Из этого примера видно, что потеря нескольких байт (неиспользуемая длина заголовка кадра в $О_{п32}$) приводит к существенной экономии машинного времени из-за отсутствия передачи поля пакета из $О_{п32}$ в $О_{повт}$.

Операция 4. Запись параметров N(S), N(R) в заголовок последнего кадра $О_{повт}$.

Операция 5. Формирование нового значения переменной передачи V(S), V(S):=V(S)+1.

Операция 6. Запись значения текущего времени $t_{тек}$. Этот параметр необходим для

работы программы $Р6_{ПД}$ – анализ необходимости перехода к передаче кадра «I» из очереди $О_{повт}$ после срабатывания таймера, указывающего на длительное неподтверждение правильного приёма кадра. Ниже приводится описание работы программы $Р6_{ПД}$. Массив кадра «I», записанный в хвост $О_{повт}$, имеет форму, приведённую на рис. 5.9.

Поля, предназначенные для включения этого кадра в $О_{повт}$, т.е. адрес предыдущего массива кадра и 0, указывающий на то, что он последний в очереди $О_{повт}$.

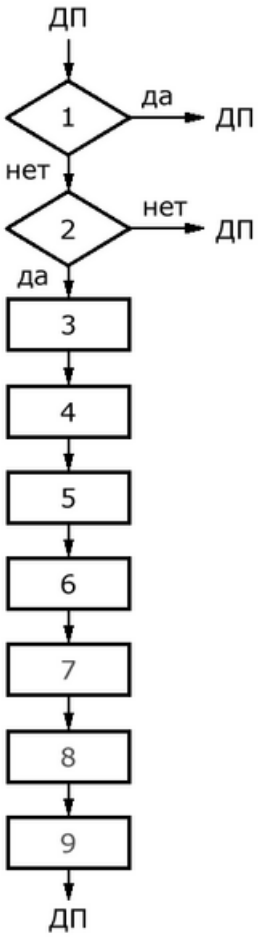


Рис. 5.8. Структурная схема программы $Р2_{ПД}$ – “Подготовка к передаче очередного «I» кадра в канал”

Рис. 5.9. Формат массива кадра “I” в $О_{повт}$

Операция 7. В регистр передачи кадра в канал переписывается заголовок кадра и пакет данных, т.е. информация с адреса $А^1$ до адреса $А^2$. Производится передача в канал этого кадра, т.е. без первых двух полей адресов (для образования списка очереди) и последнего поля $t_{тек}$ (для отслеживания тайм-аута неподтверждения – программа $Р6_{ПД}$).

Операция 8. Установить состояние “передача кадра в канал”. Это состояние снимается после передачи в канал последнего байта.

Операция 9. Снять состояние “Подготовить к передаче кадра RR в канал”, если оно было установлено. Подтверждение правильного приёма кадра «I» с противоположного конца канала ПД производится параметром N(R), передаваемом в кадре RR или в кадре «I» . Поскольку программа $Р2_{ПД}$ производит передачу кадра «I» нет необходимости передавать кадр RR, если перед этим с противоположной стороны был принят кадр «I».

5.2.3. Структурные схемы программы $Р1_{ПМ}$ - «Обработка принятых кадров «I»» и программы $Р2_{ПМ}$ – «Обработка принятого кадра RR»

Покажем работу приведенных на рис. 5.2 программ: $Р1_{ПД}$ - «Обработка принятых кадров «I»» кадра и программы $Р2_{ПМ}$ – «Обработка принятого кадра RR» (рис. 5.10).

Операция 1. Число кадров $N(О_{КПМ})$ в очереди на приём с канала равно нулю? Эта величина определяется в поле 3 характеристики очереди. Если нет, то переход к операции 2.

Операция 2. Первый кадр в $О_{КПМ}$ является информационным («I») ?

Адрес первого кадра определяется в первом поле характеристики очереди. Если да, то переход к операции 3.

Операции 3-5 выполняют функцию проверки буфера «I» кадров в очереди $О_{повт}$ с целью определения подтверждения правильного приёма «I» кадров противоположной стороной. Это производится в результате анализа параметра N(R) первого кадра в $О_{КПМ}$.

Операция 3. Число кадров $N(О_{повт})$ в очереди $О_{повт}$ не равно нулю? В случае отсутствия кадров в $О_{повт}$ программа переходит к операции 6. Операции, начиная с 6, выполняют функцию анализа параметра N(S) первого кадра «I» в $О_{КПМ}$. В случае наличия кадров в очереди $О_{повт}$ осуществляется переход к операции 4.

Операция 4. Проверка выполнения условия подтверждения правильного приёма «I»-кадров на противоположной стороне, т.е. N(S) меньше или равно N(R)-1, где N(S) – параметр в первом кадре $О_{повт}$;

Получение квитанции с параметром N(R) означает правильный приём всех кадров «I», отправленных с N(S) меньше N(R). Так как нумерация кадров производится по модулю 7 (или 127), то, например, N(R)=0 является больше N(S)=7. Аналогичное упрощение производится и далее при описании других операций и программ. Если условие N(S) меньше или равно N(R)-1 выполняется, то переход к операции 5. Это соответствует приему кадра I(0,5) на рис. 5.2.

Операция 5. Снять 1-ый кадр с $О_{повт}$ и поставить в хвост $О_{своб}$. Переход к операции 3. Цикл считывания кадров с $О_{повт}$ повторяется до тех пор, пока условия операции 3 или 4 не будет выполнено.

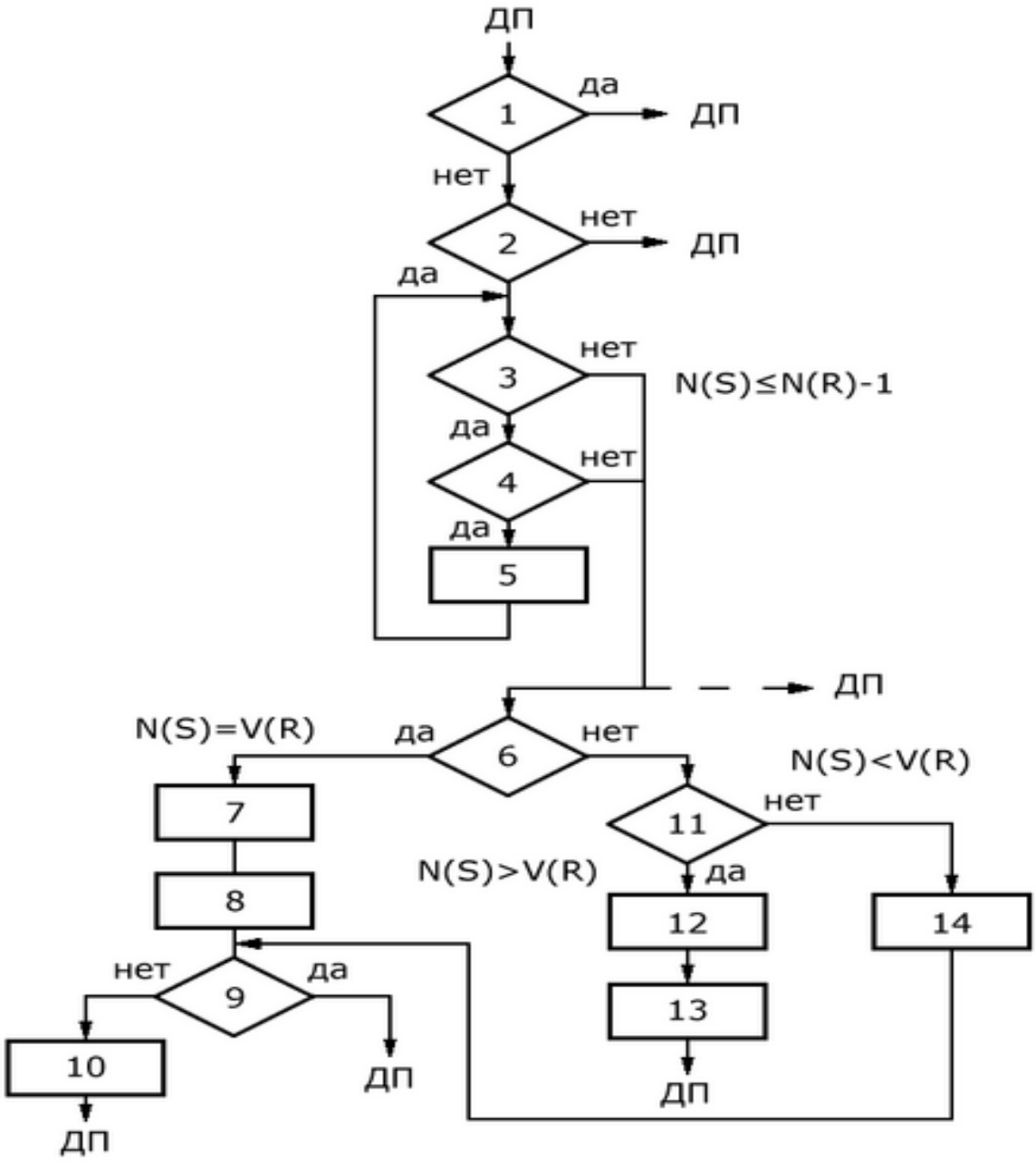


Рис. 5.10. Структурные схемы программы $P1_{ПМ}$ "Обработка принятого «I» кадра" и программы $P2_{ПМ}$ "Обработка принятого "RR" кадра"

Операция 6. Производится проверка выполнения условия N(S)=V(R), где N(S) – параметр первого кадра $O_{КПМ}$, который сравнивается с ожидаемым номером V(R). Если это условие выполняется, то производится переход к операции 7. В противном случае переход к операции 11.

Операция 7. Перенос поля данных 1-го кадра $O_{КПМ}$, т.е. пакета сетевого уровня, из

$О_{КПМ}$ в очередь пакетов для передачи на сетевой уровень. На рис. 2 эта операция соответствует приему I(0,0).

Операция 8. Формирование параметра номера следующего ожидаемого кадра «I», т.е. V(R):=V(R)+1

Операция 9. Проверить наличие пакетов на передачу в канал, т.е. $N(О_{П32})\neq 0$. Если нет пакетов, то переход к операции 10, иначе переход к ДП.

Операция 10. Установить режим «Подготовка к передаче в канал кадра RR».

Операция 11. Производится проверка выполнения условия N(S)>V(R), которая имеет место в случае неприема нескольких предыдущих кадров «I» по причине обнаружения ошибок в кадре. Если да, то переход к операции 12, иначе N(S)<V(R) и переход к операции 14.

Операция 12. Установить режим «Подготовка к передаче в канал кадра REJ».

Операция 13. Снять 1-ый кадр с $О_{КПМ}$ и поставить в хвост $О_{своб}$.

Операция 14. Эта ситуация приёма копии ранее принятого кадра «I» может иметь место при передаче с противоположной стороны кадра из очереди $О_{повт}$ по таймеру при искажении кадра RR в канале (рис. 5.11). Операция 14 снимает 1-ый кадр с $О_{КПМ}$ и ставит в хвост $О_{своб}$. После выполнения операции 14 переход к операции 9.

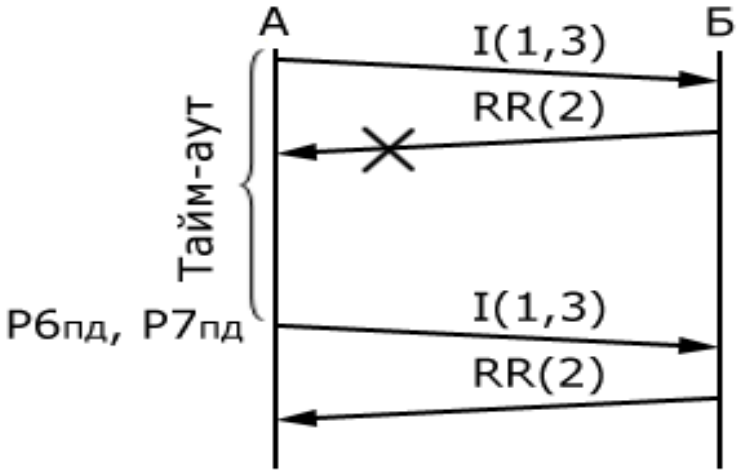


Рис. 5.11. Диаграмма приёма копии «I» кадра

5.2.4. Структурная схема программы $Р2_{ПМ}$ - «Обработка принятого кадра RR»

Покажем работу приведенной на диаграмме рис. 5.2 программы $Р2_{ПМ}$ "Обработка принятого кадра RR" (рис. 5.10).

Подтверждение правильного приема «I» кадра противоположной стороной производится с помощью параметра N(R). Этот параметр установлен в кадрах «I» и RR, поступающих с противоположной стороны.

Поэтому структурная схема программы $Р2_{ПМ}$ – «Обработка принятого кадра положительной квитанции RR» составляет часть структурной схемы программы $Р1_{ПМ}$ и включает операции 1-5 (рис. 5.10). Уточним эти операции в программе $Р2_{ПМ}$. При выполнении операции 2 производится проверка, является ли первый кадр в $О_{КПМ}$ кадром положительной квитанции RR. Если да, то переход к операции 3. Операции 3-5 производят проверку того же параметра N(R) (но кадра RR, а не кадра «I»). При невыполнении условий операции 3 или 4 производится переход к ДП, как показано прерывистой линией. При выполнении условий этих операций производится считывание подтвержденных кадров с $О_{повт}$ аналогично тому, как выполняет программа $Р1_{ПМ}$.

5.2.5. Структурные схемы программ $Р4_{ПД}$ - «Передача кадра RR» и Р5пд – «Передача

кадра REJ»

Покажем работу приведенных на диаграмме (рис. 5.2) программ $Р4_{ПД}$ - "Передача кадра RR”, $Р5_{ПД}$ - "Передача кадра REJ” (рис. 5.12).

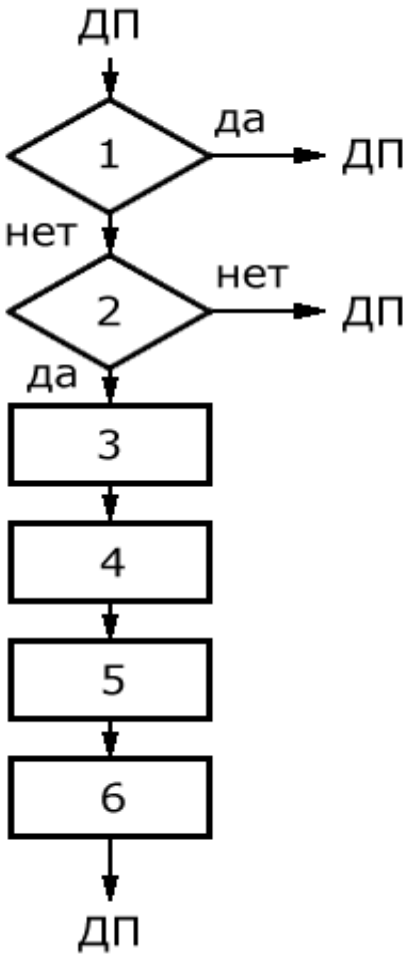


Рис. 5.12. Структурная схема $Р4_{ПД}$ "Передача кадра RR” и программы $Р5_{ПД}$ – "Передача кадра REJ”

Перед началом работы формируются шаблоны супервизорных кадров (RR, REJ), поскольку их длины фиксированы в отличие от кадра «I» . Для передачи таких типов кадров требуется установить только параметр N(R).

Приведем описание операций программы $Р4_{ПД}$, а затем отметим отличия операций для

программы $Р5_{ПД}$.

Операция 1. Состояние «Передача кадра в канал»? Если да, то переход к ДП, иначе - к операции 2.

Операция 2. Режим “Подготовка к передаче в канал кадра RR”? Этот режим устанавливается в программе $Р1_{ПМ}$. Если да, то переход к операции 3.

Операция 3. Установить значение N(R)=V(R) в шаблоне кадра RR.

Операция 4. Запись кадра RR в регистр передачи. Производится передача кадра в канал.

Операция 5. Снять режим “Подготовка к передаче в канал кадра RR”.

Операция 6. Установить состояние “Режим передачи кадра”. Это состояние так же, как и при передаче других кадров в канал сбрасывается после передачи последнего байта в канал.

В программе $Р5_{ПД}$ в операциях 2-5 вместо анализа «кадр RR» анализу подлежит «кадр REJ», а в операции 3 устанавливается значение N(R)=V(R)-1.

В программе $Р5_{ПД}$ операции 2 и 5 аналогичны программы $Р4_{ПД}$, за исключением того, что устанавливает и снимает соответственно режим «Подготовка к передаче в канал кадра REJ».

5.2.6. Структурная схема программы $Р3_{ПМ}$ - «Обработка принятого кадра отрицательной квитанции REJ»

Покажем работу приведенной на диаграмме рис.5.2 программы $Р3_{ПМ}$ – "Обработка принятого кадра отрицательной квитанции REJ” (рис. 5.13).

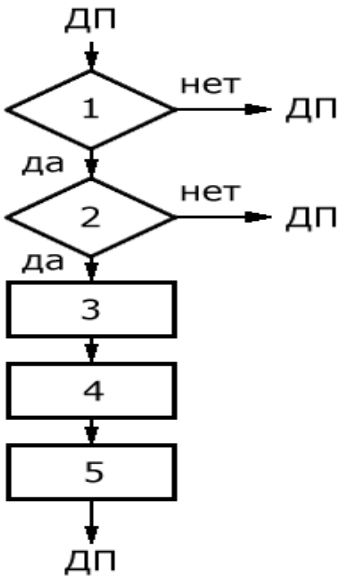


Рис. 5.13. Структурная схема программы $Р3_{ПМ}$ – "Обработка принятого кадра отрицательной квитанции REJ”

Операция 1. Число кадров в очереди на приём с канала $О_{КПМ}$ не равно нулю? (т.е. есть ли кадры в $О_{КПМ}$). Если да, то переход к операции 2.

Операция 2. Первый кадр в $О_{КПМ}$ является кадром REJ?

Операция 3. Установить режим “Передача «I» кадров с $О_{повт}$ по REJ”

Операция 4. Установить начальный адрес первого кадра $О_{повт}$ в значение текущего адреса кадра повтора $А_{тповт}$. При этом может оказаться, что N(S) кадра «I» в $О_{повт}$ меньше N(R) в кадре REJ. Повтор передачи с первого кадра $О_{повт}$ может привести к передаче уже принятых кадров «I» . Программой $Р1_{ПМ}$ они будут приняты как копии.

Операция 5. Снять первый кадр очереди $О_{КПМ}$ (т.е. REJ) и поставить его в хвост $О_{своб}$.

5.2.7. Структурная схема программы $Р3_{ПД}$ - «Подготовка к передаче «I» кадра по REJ»

Покажем работу приведенной на диаграмме рис. 5.2 программы $Р3_{ПД}$ - "Подготовка к передаче «I» кадра из очереди Оповт по REJ” (рис. 5.14).

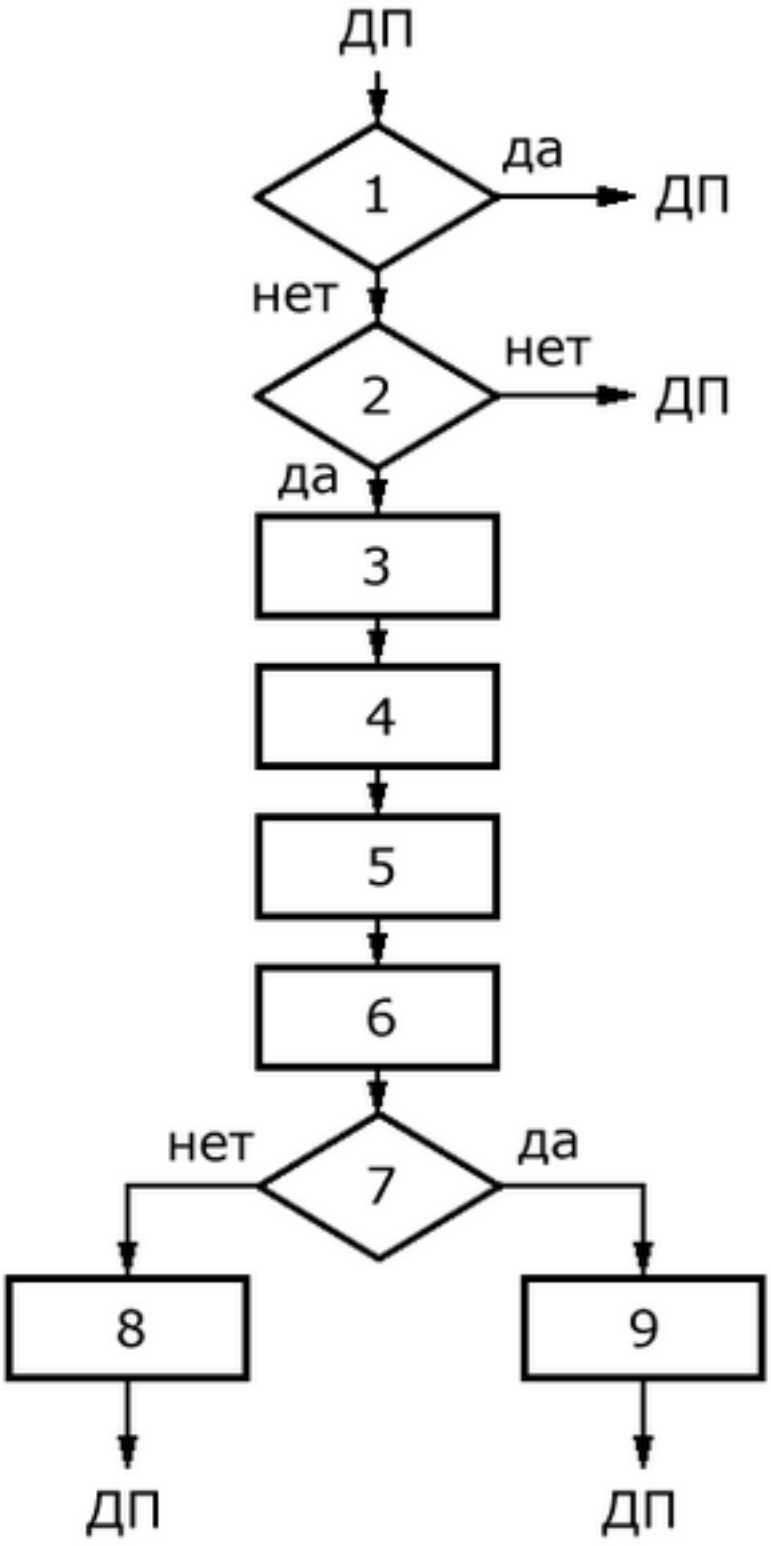


Рис. 5.14. Структурная схема программы $РЗ_{ПД}$ - "Подготовка к передаче «I» кадра по REJ”

Операция 1. Состояние “Передачи кадра в канал”?

Операция 2. Режим «Передача «I» кадров с $О_{повт}$ по REJ»? (Этот режим устанавливается предыдущей программой $Р3_{ПМ}$. при обработке принятого кадра REJ).

Операция 3. Установить в поле массива кадра по адресу $А_{тповт}$ N(R)=V(R). Эта операция по изменению N(R) в кадре $О_{повт}$ вызвана тем, что за время после передачи этого кадра в предыдущий раз, могли поступить кадры «I» с противоположного конца. Это потребует их подтверждения новым значением N(R) в кадре $О_{повт}$.

Операция 4. Установить в поле массива кадра по адресу $А_{тповт}$ значение текущего времени $t_{тек}$ передачи кадра в канал с $О_{повт}$. Эта операция аналогична операции 6 программы $Р2_{ПД}$ (см. рис. 5.8).

Операция 5. Установление состояния «Передача кадра в канал».

Операция 6. Запись кадра $О_{повт}$ из области массива кадра по адресу $А_{тповт}$ в регистр передачи в канал (т.е. без первых двух полей адресов для образования списка очереди, а также без последнего поля значения $t_{тек}$ передачи).

Операция 7. Массив кадра по адресу $А_{тповт}$ является последним в $О_{повт}$? Если нет, то переход к операции 8, иначе переход к операции 9.

Операция 8. Установление $А_{тповт}$ следующего в очереди $О_{повт}$ кадра.

Операция 9. Снятие режима передачи кадра с $О_{повт}$ по REJ.

5.2.8. Структурная схема программы $Р6_{ПД}$ - «Анализ перехода в режим повторения передачи кадра по таймеру»

Покажем работу приведенной на диаграмме рис. 5.11 программы $Р6_{ПД}$ - «Анализ перехода в режим повторения передачи кадра «I» по таймеру» (рис. 5.15).

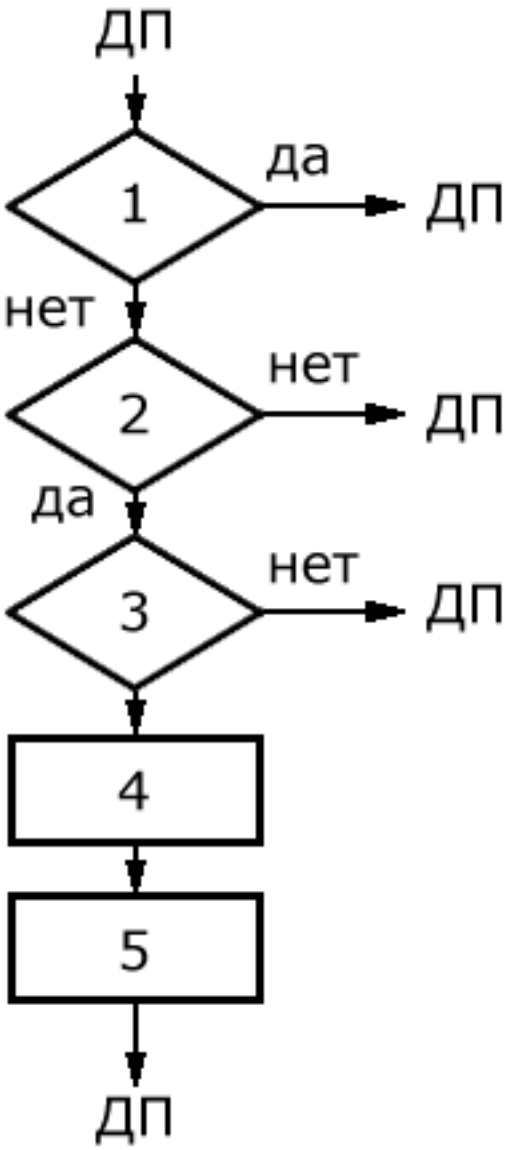


Рис. 5.15. Структурная схема программы $Р6_{ПД}$ – "Анализ перехода в режим повторения передачи «I» кадра по таймеру"

Операция 1. Состояние "Передача кадра в канал?"

Операция 2. Режим "Передача очередного кадра в канал?"

Операция 3. Проверить «Истекло ли допустимое время ожидания подтверждения кадра в $О_{повт}$ после его передачи в канал? Это время находится в поле массива кадра $О_{повт}$ и сравнивается с текущим временем. Если это время меньше допустимого по таймауту, то выход к ДП. В противном случае переход к операции 4. Эта операция

производится по всем кадрам $О_{повт}$.

Операция 4. Установка режима "Повтор кадра из $О_{повт}$ по таймеру". Установить начальный адрес массива кадра $А_{тповт}$, подлежащего повтору.

Операция 5. Сброс состояния "Передача очередного кадра в канал".

5.2.9. Структурная схема программы $Р7_{ПД}$ - «Подготовка к передаче «I» кадра по таймеру»

Покажем работу приведенной на диаграмме рис. 5.11 программы $Р7_{ПД}$ - «Подготовка к передаче «I» кадра по таймеру" (рис. 5.16).

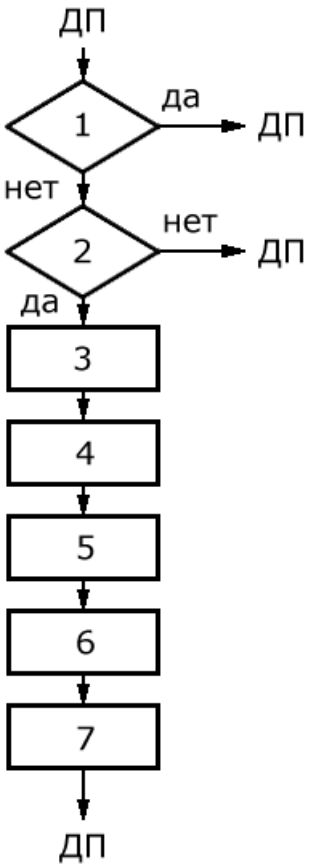


Рис. 5.16. Структурная схема программы $Р7_{ПД}$ - "Подготовка к передачи «I» кадра по таймеру"

Операция 1. «Состояние передачи кадра в канал?»

Операция 2. Состояние режима «повторение кадра из $О_{повт}$ по таймеру»?

Операции 3-5. Осуществляют подготовку и пересылку в регистр передачи в канал кадра из $О_{повт}$ с начальным адресом массива этого кадра $А_{тповт}$.

Операция 3. Установить в поле массива передаваемого кадра $О_{повт}$ N(R)=V(R) (см. операцию 3 в $Р3_{ПД}$).

Операция 4. Установить в поле массива передаваемого кадра $О_{повт}$ $t_{тек}$ передачи кадра в канал из $О_{повт}$.

Операция 5. Запись передаваемого кадра из $О_{повт}$ из области массива первого кадра (без первых двух полей адресов для образования списка очереди, а также последнего поля-значения $t_{тек}$ передачи) в регистр передачи в канал.

Операция 6. Установление состояния «передача кадра в канал».

Операция 7. Снятие состояния режим «повторение кадра из $О_{повт}$ по таймеру».

5.2.10. Структурная схема программы $Р4_{ПМ}$ - «Установление и снятие запрета на передачу «I» кадров»

В соответствии с рекомендацией МСЭ-Т X25 одной из причин приёма супервизорного кадра неготовность к приему RNR (receive not ready) может быть сообщение противоположной стороны о перегрузке. Также как и другие супервизорные кадры, RNR включает параметр N(R) для снятия из $О_{повт}$ на противоположной стороне правильно принятых «I» кадров. Покажем работу программы $Р4_{ПМ}$ - "Установление и снятие запрета на передачу «I» кадров (рис. 5.17).

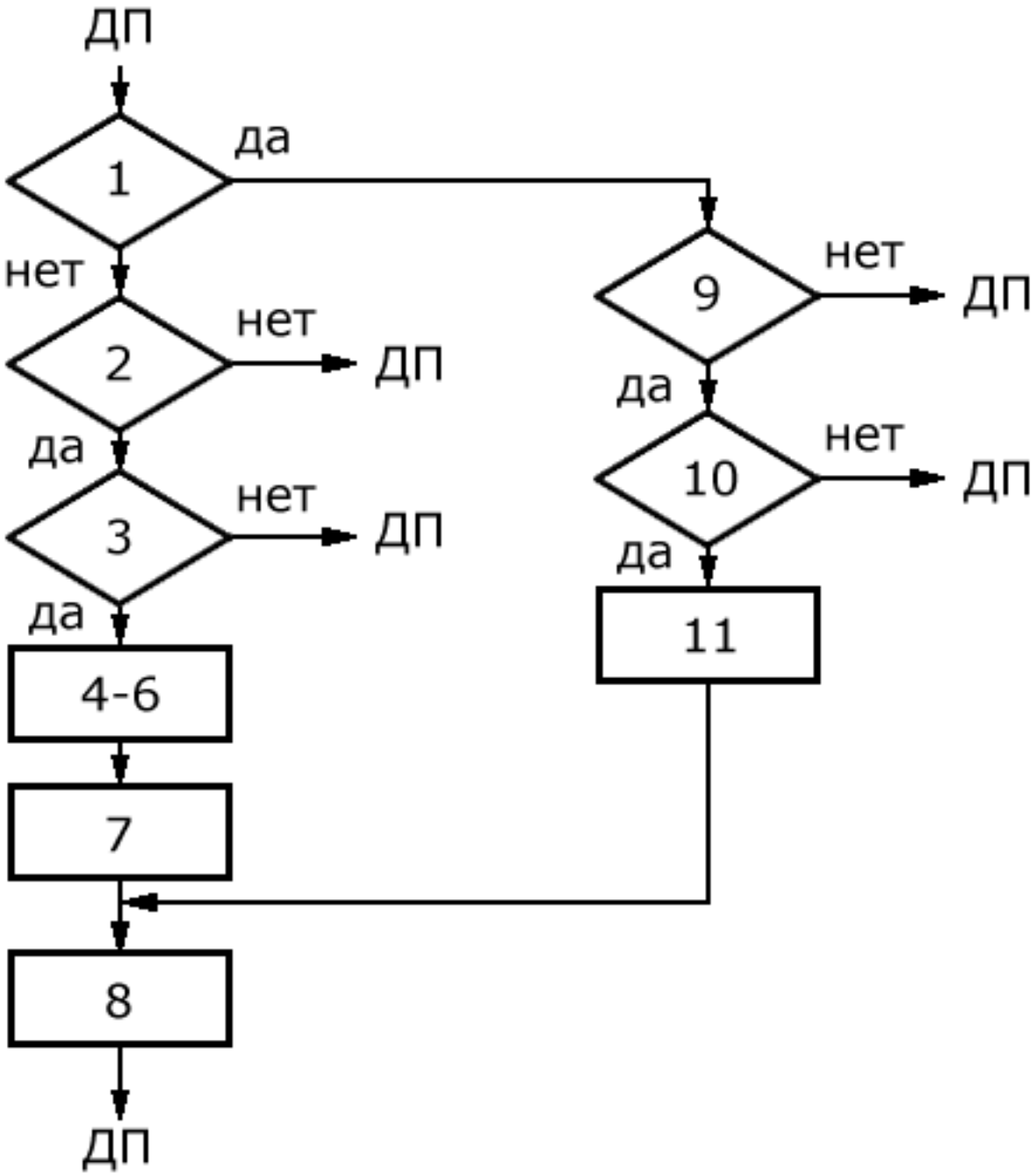


Рис. 5.17. Структурная схема программы $Р4_{ПМ}$ - "Установление и снятие запрета на передачу «I» кадров

Операция 1. Состояние "запрет на передачу кадра"?

Операция 2. Число кадров в очереди на приём из канала $О_{КПМ}$ не равно нулю?

Операция 3. Первый кадр в $О_{КПМ}$ является RNR?

На рис. 17 приведена структурная схема программы $Р4_{ПМ}$ - «Установление и снятие запрета

на передачу «I» кадров». Операция 4-6. Выполняют функцию по снятию из $О_{повт}$ подтвержденных «I» кадров. Эта операция проводится на основании параметра N(R), входящего в кадр RNR и аналогична программе Р2пм по приёму кадра RR.

Операция 7. Установить состояние "Запрет на передачу кадра".

Операция 8. Поставить первый кадр из $О_{КПМ}$ в $О_{своб}$.

Операция 9. Число кадров $О_{КПМ}$ ноль?

Операция 10. В $О_{КПМ}$ первый кадр является RR?

Операция 11. Сброс состояния "Запрет на передачу кадров". Если имеет место состояние "Запрет на передачу кадра", установленное операцией 7, то диспетчер программ не передаёт управление ни одной из фоновых программ передачи $Р1_{ПД}$ $Р7_{ПД}$. Для упрощения этих структурных схем операция проверки условия «Запрет на передачу кадра не приводится».

Дополнение. Алгоритмы реализации программ для использования в лабораторных работах

Настоящее дополнение включает предлагаемые алгоритмы реализации шести программ для использования в лабораторных работах.

Лабораторная работа №1

Алгоритм программы формирования и передачи в канал связи очередного информационного кадра

(см. главы 4,5)

Программа LAB1

Описание:

-константы N1, N2, Z1, Z2, *m*; исходные данные для 5 вариантов лабораторной работы и контрольного примера приведены в разделе 1.6.

- переменные D, V(S), V(R), N(S), N(R), *n*;

- программы DISP1, P_1, P_2, P_3, P_4, P_5;

- очереди $O_{п32}$, $O_{повт}$, $O_{своб.}$

Диспетчер программы DISP1

Begin;

D:= 1

IF D = 1 THEN GO TO P_1 ELSE IF D = 2 THEN GO TO P_2 ELSE

IF D= 3 THEN GO TO P_3 ELSE IF D = 4 THEN GO TO P_4 ELSE

IF D = 5 THEN GO TO P_5 ELSE

END

Программы:

P_1 – формирование очереди из N1 свободных блоков;

P_2 – формирование N2 пакетов данных;

P_3 – перенос N2 пакетов данных из очереди $O_{своб}$ в очередь пакетов $O_{п32;}$

P_4 – формирование информационного кадра, включающего первый пакет в очереди пакетов $O_{п32;}$

P_5 – перенос информационного кадра, сформированного программой P_4, в очередь повтора $О_{повт}$ и в регистр на передачу в канал.

По окончании работы программы P_5 необходимо показать результат: содержание полей в побитовой и десятичной форме находящегося в $О_{повт}$ кадра (N(S), N(R) и тип кадра в заголовке кадра и информационной части входящего в него пакета).
Разработать программу, выполняющую функцию с формальными аргументами переноса массива первого блока из одной очереди в конец другой очереди. На основании приведенного ниже алгоритма выполнить программы P_3 и P_5, используя эту программу с фактическими параметрами.

1.1. Программа P_1

а) Выделение памяти под N1 свободных блоков (3<= N1=< 20). Каждый свободный блок занимает 138 байт:

- 2 байта под адрес предыдущего блока в списке блоков (первое адресное поле связки очереди);
- 2 байта под адрес следующего блока в списке блоков (второе адресное поле связки очереди);
- 3 байта под заголовок пакета;
- 1 байт под заголовок кадра;
- 128 байт под информационную часть пакета данных;
- 2 байта под контрольно-проверочную комбинацию КПК.

Очистить память, занятую свободными блоками.

б) Установление адресов связки в N1 свободных блоках:

- выделить память под характеристику очереди свободных блоков $Н_{своб}$ с начальным адресом $АН_{своб.}$ Установить поля характеристики $Н_{своб}$ (рис.1).

$АН_{своб}$

A(1)	A(N1)	N1

Рис.1. Характеристика $Н_{своб}$

Здесь

A(1) – адрес начала массива первого свободного блока в очереди $О_{своб.}$

A(N1) – адрес начала массива последнего свободного блока в очереди $О_{своб.}$

Под массивом блока будем понимать блок (пакет, кадр, ячейка и др.) с адресными полями связки очереди.

Установить адресные поля связки первого (рис. 2а) и N1 – го (рис. 2б) свободного блока в очереди $О_{своб.}$

A(1)

0	A(N1)	

а)

A(N1)

A(N1) -1	0	

б)

Рис. 2. Формат первого (а) и последнего (б) свободного блока в списке очереди $О_{своб}$

Установить адреса связки всех свободных блоков, кроме первого и последнего.

FOR i=2, 3 …. (N1-1) DO

Запись в первое адресное поле i-го блока адрес начала i-1 блока списка очереди;

Запись во второе адресное поле i-го блока адрес начала i+1 блока списка очереди.

i=i+1

D:=D+1

GO TO DISP1

1.2. Программа P_2

Записать данные в информационную часть первых N2 свободных блоков очереди $О_{своб,}$ т.е. сформировать пакет данных в этих свободных блоках. Для упрощения примем заголовок пакета равным нулю. На рис. 3 показан формат размещенного пакета в свободном блоке с начальным адресом A(i).

байты	2	2	1	3	128	2
Начальный адрес A(i)	Первое адресное	Второе адресное		Заголовок пакета	Информационная часть пакета	

	поле	поле				

Рис. 3. Формат размещения пакета данных в свободном блоке с начальным адресом A(i)

n:=*m*

FOR i= 1,2…..N2 DO

Записать s в поле информационной части пакета с начальным адресом массива A(i).

n:=*n*+1

END

В результате в первых N2 свободных блоках установлены пакеты данных, образуя очередь пакетов $О_{п32.}$ Функция следующей программы **$Р_3$** в освобождении $О_{своб}$ от пакетов очереди пакетов $О_{п32}$ (перенос их из . $О_{своб}$ в $О_{п32}$), формирование характеристики очереди пакетов $О_{п32.}$

D:=D+1

GO TO DISP1

1.3. Программа $Р_3$

Выделить память под характеристику $Н_{п32}$ очереди пакетов $О_{п32}$ с начальным адресом $АН_{п32.}$ Установить поля характеристики $Н_{п32}$ (рис 4).

$АН_{п32}$

A(1)	A(N2)	N2

Рис.4. Характеристика $Н_{п32}$

Установить значение ноль во втором адресном поле пакета N2, т.е. адрес следующего блока в списке очереди.

Откорректировать поля характеристики очереди очереди свободных блоков $Н_{своб}$ (рис.5).

$АН_{своб}$

A(N2+1)	A(N1)	N1- N2

Рис.5. Характеристика $Н_{своб}$

Установить значение ноль в первом адресном поле массива свободных блоков с адресом

A(N2+1) т.е. адрес предыдущего блока в списке очереди.

D:=D+1

GO TO DISP1

1.4. Программа P_4

Сформировать кадр с входящим в него первым в очереди пакетов $О_{п32}$ пакетом данных. Начальный адрес массива этого кадра A(1). На рис. 6 показан формат его полей.

байты	2	2	1	3	128	2
Начальный адрес массива A(1)	Первое адресное поле - 0	Второе адресное поле - A(2)	Заголо-вок кадра	Заголо-вок пакета	Информационная часть пакета	КПК

…адресная часть ….. …… кадр …….

……. пакет ……. ……

Рис.6. Формат полей массива информационного кадра “I” с начальным адресом A(1)

Установить исходные состояния: V(S):= Z1. (0<= V(S)=< 7).

Установить параметры информационного кадра: N(S):=V(S);

V(S):=V(S)+1.

Формирование полей заголовка (длиной 8 бит) информационного кадра “I” с начальным адресом массива A(1):

- определить V(R) по исходным данным Z2 разд. 1.6 (0<= V(R)=< 7), ожидаемый противоположной стороной подтверждения переданных им кадров “I” , т.е. приема кадра “I” с ожидаемым N(S). V(R) := Z2;
- записать биты заголовка <2-4>:= N(S), биты N(R) заголовка <6-8>:= V(R), бит заголовка <1>:= 0 (тип кадра – информационный).
- сформировать контрольно-проверочную комбинацию КПК кадра: произвести сложение по

модулю 2 всех байт кадра и занести результат в поле КПК (см. рис.5).

D:=D+1
GO TO DISP1

1.5. Программа P_5

Перенос информационного кадра “I” с начальным адресом массива A(1) из очереди $О_{п32}$ в конец очереди $О_{повт}$:

- выделить память под характеристику $Н_{повт}$ очереди пакетов $О_{повт}$ с начальным адресом $АН_{повт.}$ Установить поля характеристики $Н_{повт}$ (рис. 7);

$АН_{повт}$

A(1)	A(1)	1

Рис.7. Характеристика $Н_{повт}$

- установить второе адресное поле массива информационного кадра “I” с начальным адресом A(1) в ноль (см. рис.6);
- откорректировать характеристику очереди пакетов $О_{п32}$, т.е. $Н_{п32}$ (рис.8). Сравните с рис.4.

$АН_{п32}$

A(2)	A(N2)	N2-1

Рис.8. Характеристика $Н_{п32}$

- установить первое адресное поле массива очереди пакетов данных $О_{п32}$ в ноль.

Перенести кадр “I” в выходной регистр передачи $RG_{вых}$ в канал связи. Передать в канал этот кадр из регистра $RG_{вых.}$ Очистить регистр $RG_{вых.}$

1.6 Исходные данные для лабораторной работы

В таблице 1 приведены исходные данные пяти вариантов лабораторной работы и контрольного примера.

Таблица 1. Исходные данные для лабораторной работы

Параметр	1 вариант	2 вариант	3 вариант	4 вариант	5 вариант	Контрольный пример

N1	15	14	13	12	11	20
N2	7	6	5	4	3	8
Z1	0	1	3	4	5	2
Z2	0	3	2	4	5	1
m	2	3	4	5	6	1

Ниже приведены некоторые характеристики контрольного примера.

$АН_{своб}$

A(1)	A(20)	20

Рис.1. Характеристика $Н_{своб}$

A(1)

0	A(20)	

а)

A(20)

A(20)-1	0	

б)

Рис. 2. Формат первого (а) и последнего (б) свободного блока в списке очереди $О_{своб}$

$АН_{п32}$

A(1)	A(8)	8

Рис.4. Характеристика $Н_{п32}$

$АН_{своб}$

A(9)	A(20)	12

Рис.5. Характеристика $Н_{своб}$

байты	2	2	1	3	128	2
Начальный	Первое	Второе	Заголовок	Заголо-	Информационная	КПК

адрес массива А(1)	адресное поле - 0	адресное поле - А(2)	кадра – 00100100	вок пакета - все 0	часть пакета - 10	00100110

…адресная часть … …… кадр ……..

..… пакет ……. ……..

Рис.6. Формат полей массива информационного кадра “I” с начальным адресом А(1)

$АН_{п32}$

А(2)	А(8)	7

Рис.8. Характеристика $Н_{п32}$

Лабораторная работа №2

Алгоритм программы приема с канала кадра “RR”

(см. главы 4,5)

Реализация алгоритма программы приема с канала кадра “RR” предусматривает последовательное выполнение программы LAB1 (лабораторная работа 1) и программы LAB2, алгоритм которой приводится ниже.

Программа LAB2

Описание:

-константы N1, N2; исходные данные для 5 вариантов лабораторной работы и контрольного примера приведены в разделе 1.6. лаб. 1.

- переменные D,V(R), N(R), REGIM;
- программы DISP2, P_6, P_7, P_8, P_9, P_{10}, P_{11};
- очереди $O_{кпм}$, $O_{своб.}$.

Диспетчер программы DISP2

Begin

D := 1

IF D = 1 THEN GO TO P_6 ELSE IF D = 2 THEN GO TO P_7 ELSE

IF D = 3 THEN GO TO P_8 ELSE IF D = 4 THEN GO TO P_9 ELSE

IF D= 5 THEN GO TO P_{10} ELSE IF D= 6 THEN GO TO P_{11} ELSE

END

Программы:

P_6 – формирование принятого кадра “RR”, подтверждающего правильный прием переданного на противоположную сторону информационного кадра “I” (см. лаб. 1). Проверка безошибочного приема кадра RR с канала связи;

P_7 – запись этого кадра RR с контрольно-проверочной комбинацией КПК в первый блок очереди $O_{своб}$;

P_8 – перенос принятого кадра RR из $O_{своб}$ в очередь $O_{кпм}$;

P_9 – проверка правильного приема переданного ранее кадра “I” и находящегося в очереди

повтора $О_{повт}$;

$Р_{10}$ – считывание кадров “RR” из очереди $О_{кпм}$ и “I” из $О_{повт}$ и установка их в очередь $О_{своб}$;

$Р_{11}$ – установление режима передачи очередного информационного кадра “I” в канал.

По окончании работы программы $Р_{11}$ необходимо показать результат: содержание в побитовой и десятичной форме полей последнего и предпоследнего кадров в очереди $О_{своб.}$ Показать промежуточные данные - заголовки этих кадров перед переносом их в $О_{своб.}$

Примечание. В настоящей и всех остальных лабораторных работах (включая лабораторные работы в разделе дополнения к главе 7) рекомендуется использовать разработанную в разд. 6.1 программу, выполняющую функцию с формальными аргументами переноса массива первого блока из одной очереди в конец другой очереди. Это упрощает выполнение всех лабораторных работ.

2.1. Программа $Р_6$

Выделение памяти для формирования принятого кадра RR, подтверждающего правильный прием переданного на противоположную сторону кадра “I” (лаб. работа 1). На рис.1 приведен этот формат, включающий 1 байт кадра RR и 2 байта КПК этого кадра. Начальный адрес этого кадра с КПК - $А(RG_{вх})$. Он имитирует входной регистр с канала $RG_{вх}$, в котором в действительности аппаратным образом проверяется с помощью КПК был ли искажен кадр в канале. Как видно из рис.1 регистр состоит из трех байтов.

$А(RG_{вх})$

Биты	8	7	6	5	4	3	2	1	16 бит КПК
Значения	0	1	1	0	0	0	0	1	старший байт – все нули младший байт - 01100001

…..N(R)…… …тип кадра…….

Рис. 1. Формат принятого кадра RR с КПК во входной регистр с начальным адресом $А(RG_{вх})$

Сформировать поля принятого кадра (значения приведены для контрольного примера):

- установить тип кадра RR - биты кадра <1-4>:= 0001;
- установить N(R) в биты кадра RR <6-8>:= 011. Это значение N (R) равно значению N(S)+1, где N(S) является параметром переданного ранее кадра “I” и находящегося в очереди $О_{повт}$ (лаб. работа 1). Для контрольного примера N(S)=2. Значит N(R) в кадре RR равен 3, что

отражено на рис. 1;

- установить КПК (старший байт равен нулю, младший байт – значение кадра RR (01100001). Это означает, что кадр RR принят неискаженным в канале.

D:=D+1
GO TO DISP2

2.2. Программа P_7

Записать в массив первого блока по адресу A(N2+1) очереди свободных блоков $O_{своб}$ принятый с канала связи кадр RR, подтверждающий правильный прием информационного кадра “I” (поэтому в кадре отсутствует КПК).

Значения полей принятого кадра приведены для контрольного примера на рис.2.

A(N2+1)

Биты	16 бит	16 бит	8	7	6	5	4	3	2	1
Значения	0	0	0	1	1	0	0	0	0	1

….адр. часть…… ….кадр RR …….

Рис. 2. Кадр RR в массиве очереди свободных блоков $O_{своб}$

Откорректировать поля характеристики $H_{своб}$ очереди свободных блоков $O_{своб}$, т.е. снять свободный блок с начальным адресом массива по A(N2+1) из очереди свободных блоков $O_{своб}$ (рис.3).

$AH_{своб}$

A(N2+2)	A(N1)	N1- N2 -1

Рис.3. Характеристика $H_{своб}$

Установить в ноль первое адресное поле первого массива свободного блока очереди свободных блоков $O_{своб}$ с начальным адресом A(N2+2).

D:=D+1
GO TO DISP2

2.3. Программа P_8

Переписать из очереди свободных блоков $О_{своб}$ кадр RR (в массиве кадра с начальным адресом A(N2+1)) в очередь принятых с канала кадров $О_{кпм.}$ (для упрощения рассматривается исходное состояние отсутствия кадров в очереди $О_{кпм.}$):

- выделить память под характеристику $Н_{кпм..}$ очереди принятых кадров $О_{кпм..}$ с начальным адресом $АН_{кпм.}$ Установить поля характеристики $Н_{кпм}$ (рис 3) - поставить в очередь $О_{кпм}$ массив кадра с начальным адресом A(N2+1);

$АН_{кпм}$

A(N2+1)	A(N2+1)	1

Рис.4. Характеристика $Н_{кпм}$

- установить значение ноль в оба адресные поля массива кадра с начальным адресом A(N2+1).

D:=D+1
GO TO DISP2

2.4. Программа $Р_9$

IF N(R) принятого кадра RR (биты <6-8> -1, рис. 1) = N(S).
Здесь N(S) является параметром переданного ранее кадра “I” и находящийся первым в очереди $О_{повт}$ (лаб. работа 1)
THEN END ELSE OSHIBKA

Программой $Р_6$ это условие выполняется. Для контрольного примера N(S)=2.

D:=D+1
GO TO DISP2

2.5. Программа $Р_{10}$

Поставить кадр RR с начальным адресом массива A(N2+1) из очереди принятых с канала кадров $О_{кпм}$ в конец очереди свободных блоков $О_{своб,}$ при этом очистив его (кроме адресных полей). Откорректировать поля характеристики очереди $Н_{своб}$ (рис.5).

$АН_{своб}$

A(N2+2)	A(N2+1)	N1- N2

Рис.5. Характеристика $Н_{своб}$

Установить в массиве с начальным адресом A(N2+1) очереди свободных блоков $О_{своб}$ в первом адресном поле значение A(N1) и ноль во втором адресном поле.

Установить в массиве с начальным адресом A(N1) очереди свободных блоков $О_{своб}$ во втором адресное поле значение A(N2+1).

Поставить массив информационного кадра “I” с начальным адресом A(1) массива очереди $О_{повт}$ в конец очереди свободных блоков $О_{своб,}$ предварительно очистив его (кроме адресных полей). Откорректировать поля характеристики очереди $Н_{своб}$ (рис.6).

$АН_{своб}$

A(N2+2)	A(1)	N1- N2+1

Рис.6. Характеристика $Н_{своб}$

Установить значение A(N2+1) в первом адресном поле и ноль во втором адресном поле массива с начальным адресом A(1) очереди свободных блоков $О_{своб.}$

Установить значение A(1) во втором адресном поле массива с начальным адресом A(N2+1) очереди свободных блоков $О_{своб.}$

Установить в ноль поля характеристик очереди $О_{повт}$ (по адресу $АН_{повт.}$) и $О_{кпм}$ (по адресу $АН_{кпм}$).

D:=D+1
GO TO DISP2

2.6. Программа $Р_{11}$

Установление режима передачи очередного информационного кадра “I” в канал.

REGIM:=1 (передача в канал очередного кадра “I”)

D:=D+1
GO TO DISP2

2.7. Некоторые характеристики контрольного примера

$АН_{своб}$

A(10)	A(20)	11

Рис.3. Характеристика $Н_{своб}$

$АН_{кпм}$

A(9)	A(9)	1

Рис.4. Характеристика $Н_{кпм}$

$АН_{своб}$

A(10)	A(9)	12

Рис.5. Характеристика $Н_{своб}$

$АН_{своб}$

A(10)	A(1)	13

Рис.6. Характеристика $Н_{своб}$

Лабораторная работа №3

Алгоритм программы передачи в канал связи нескольких информационных кадров

(см. главы 4,5)

Программа LAB3
Описание:

-константы N1, N2, Z1, Z2, *m*, *n*, MCICL; исходные данные для 5 вариантов лабораторной работы и контрольного примера приведены в разделе 3.6.

- переменные D, V(S), V(R), N(S), N(R), *n* ,CICL, REGIM;

- программы DISP3, P_1, P_2, P_3, P_4, P_5;

- очереди $O_{п32}$, $O_{повт}$, $O_{своб.}$

Begin
REGIM:=1 (передача в канал очередного кадра “I”)
END

Диспетчер программы DISP3
IF REGIM=1 THEN DISP3 ELSE END ; переход к программе DISP3

CICL:=1

Begin;

D:= 1

IF D = 1 THEN GO TO P_1 ELSE IF D = 2 THEN GO TO P_2 ELSE

IF D= 3 THEN GO TO P_3 ELSE IF D = 4 THEN GO TO P_4 ELSE

IF D = 5 THEN GO TO P_5 ELSE

END

Программы:

P_1 – формирование очереди из N1 свободных блоков;

P_2 – формирование N2 пакетов данных;

P_3 – перенос N2 пакетов данных из очереди $O_{своб}$ в очередь пакетов $O_{п32;}$

P_4 – формирование массивов MCICL информационных кадров с входящими в него пакетами в очереди пакетов $O_{п32}$ пакетов данных;

P_5 – перенос информационных кадров MCICL, сформированных программой P_4, в очередь повтора $O_{повт}$ и в регистр на передачу в канал.

По окончании работы программы P_5 необходимо показать результат: содержание полей в побитовой и десятичной форме всех находящихся в $О_{повт}$ информационных кадров (заголовка кадра и информационной части входящего в него пакета).

3.1. Программа P_1

а) Выделение памяти под N1 свободных блоков (3<= N1=< 20). Каждый свободный блок занимает 138 байт:

- 2 байта под адрес предыдущего блока в списке блоков (первое адресное поле связки очереди);
- 2 байта под адрес следующего блока в списке блоков (второе адресное поле связки очереди);
- 3 байта под заголовок пакета;
- 1 байт под заголовок кадра;
- 128 байт под информационную часть пакета данных;
- 2 байта под контрольно-проверочную комбинацию КПК.

Очистить память, занятую свободными блоками.

б) Установление адресов связки в N1 свободных блоках:

- выделить память под характеристику очереди свободных блоков $Н_{своб}$ с начальным адресом $АН_{своб.}$ Установить поля характеристики $Н_{своб}$ (рис.1).

$АН_{своб}$

A(1)	A(N1)	N1

Рис.1. Характеристика $Н_{своб}$

Здесь

A(1) – адрес начала массива первого свободного блока в очереди $О_{своб;}$

A(N1) – адрес начала массива последнего свободного блока в очереди $О_{своб.}$

Под массивом блока будем понимать блок (пакет, кадр, ячейка и др.) с адресными полями связки очереди.

Установить адресные поля связки первого (рис. 2а) и N1 – го (рис. 2б) свободного блока в очереди $О_{своб.}$

A(1)

0	A(N1)	

а)

A(N1)

A(N1)-1	0	

б)

Рис. 2. Формат первого (а) и последнего (б) свободного блока в списке очереди $О_{своб}$

Установить адреса связки всех свободных блоков, кроме первого и последнего

FOR i=2, 3 …. (N1-1) DO
Запись в первое адресное поле i-го блока адрес начала i-1 блока списка очереди;

Запись во второе адресное поле i-го блока адрес начала i+1 блока списка очереди.

i=i+1

D:=D+1

GO TO DISP3

3.2. Программа $Р_2$

Записать данные в информационную часть первых N2 свободных блоков очереди $О_{своб,}$ т.е. сформировать пакет данных в этих свободных блоках. Для упрощения примем заголовок пакета равным нулю.

На рис. 3 показан формат размещенного пакета в свободном блоке с начальным адресом A(i).

байты	2	2	1	3	128	2
Начальный адрес A(i)	Первое адресное поле	Второе адресное поле		Заголовок пакета	Информационная часть пакета	

Рис. 3. Формат размещения пакета данных в свободном блоке с начальным адресом A(i).

n:=*m*

FOR i= 1,2…..N2 DO

Записать *n* в поле информационной части пакета с начальным адресом массива A(i).

n:=*n*+1

END

В результате в первых N2 свободных блоках установлены пакеты данных, образуя очередь пакетов $О_{п32.}$

D:=D+1

GO TO DISP3

3.3. Программа $Р_3$

Освободить $О_{своб}$ от пакетов очереди пакетов $О_{п32}$ (перенос их из . $О_{своб}$ в $О_{п32}$). Сформировать характеристику очереди пакетов $О_{п32.}$

Выделить память под характеристику $Н_{п32}$ очереди пакетов $О_{п32}$ с начальным адресом $АН_{п32.}$

Установить поля характеристики $Н_{п32}$ (рис 4).

IF CICL=1 THEN

$АН_{п32}$

A(1)	A(N2)	N2

Рис.4. Характеристика $Н_{п32}$

- установить значение ноль во втором адресном поле пакета N2, т.е. адрес следующего блока в списке очереди.

ELSE

Откорректировать поля характеристики очереди $Н_{своб}$ (очереди свободных блоков $О_{своб}$), рис.5.

$АН_{своб}$

A(N2+1)	A(N1)	N1- N2

Рис.5. Характеристика $Н_{своб}$

Установить значение ноль в первом адресном поле массива свободных блоков с адресом A(N2+1) т.е. адрес предыдущего блока в списке очереди.

D:=D+1
GO TO DISP3

3.4. Программа $Р_4$

Сформировать массивы MCICL кадров с входящими в него пакетами в очереди пакетов $О_{п32}$ пакетов данных. На рис. 6 показаны форматы полей.

байты	2	2	1	3	128	2
Начальный адрес массива A(CICL)	Первое адресное поле	Второе адресное поле	Заголо-вок кадра	Заголо-вок пакета	Информационная часть пакета	КПК

…адресная часть ….. …… кадр ……

……. пакет …….

Рис.6. Формат полей массива MCICL информационных кадров “I”

Установить исходные состояния: V(S):= Z1. (0<= V(S)=< 7),
V(R):= Z2

FOR CICL = 1, 2... MCICL DO

- установить параметры информационного кадра: N(S):=V(S);
V(S):=V(S)+1
Формирование полей заголовка (длиной 8 бит) информационного кадра “I” с начальным адресом массива A(CICL) - биты заголовка <2-4>:= N(S), биты N(R) заголовка <6-8>:= V(R), бит заголовка <1>:= 0 (тип кадра – информационный).
Сформировать контрольно-проверочную комбинацию КПК кадра: произвести сложение по модулю 2 всех байт кадра и занести результат в поле КПК (см. рис.5)

END
D:=D+1

GO TO DISP3

3.5. Программа P_5

Перенос массивов первых MCICL информационных кадров “I” из очереди $О_{п32}$ в очередь $О_{повт}$:

- выделить память под характеристику $Н_{повт}$ очереди пакетов $О_{повт}$ с начальным адресом $АН_{повт.}$ Установить поля характеристики $Н_{повт}$ (рис. 7);

$АН_{повт}$

A(1)	A(MCICL)	MCICL

Рис.7. Характеристика $Н_{повт}$

- установить в ноль второе поле массива очереди пакетов $О_{повт}$ по адресу A(MCICL).

- откорректировать характеристику очереди пакетов $О_{п32}$, т.е. $Н_{п32}$ (рис.8). Сравните с рис.4.

$АН_{п32}$

A(MCICL+1)	A(N2)	N2-MCICL

Рис.8. Характеристика $Н_{п32}$

- установить первое адресное поле A(MCICL+1) массива очереди пакетов данных $О_{п32}$ в ноль

Перенести кадры “I” в выходной регистр передачи $RG_{вых}$ в канал связи. Передать в канал этот кадр из регистра $RG_{вых.}$ Очистить регистр $RG_{вых.}$

D:=D+1
GO TO DISP3

3.6. Исходные данные для лабораторной работы

В таблице 1 приведены исходные данные пяти вариантов лабораторной работы и контрольного примера.

Таблица 1. Исходные данные для лабораторной работ

Параметр	1 вариант	2 вариант	3 вариант	4 вариант	5 вариант	Контрольный вариант
N1	15	14	13	12	11	20
N2	7	7	7	7	7	8
Z1	0	2	1	3	3	2
Z2	0	3	2	4	5	1
m	2	3	4	5	6	1
MCICL	4	3	4	4	4	3

Некоторые характеристики контрольного примера

$АН_{своб}$

A(1)	A(20)	20

Рис.1. Характеристика $Н_{своб}$

A(1)

0	A(20)	

а)

A(20)

A(20) -1	0	

Рис. 2. Формат первого (а) и последнего (б) массива свободного блока в списке очереди $О_{своб}$

$АН_{п32}$

A(1)	A(8)	8

Рис.4. Характеристика $Н_{п32}$

$АН_{своб}$

A(9)	A(20)	12

Рис.5. Характеристика $Н_{своб}$

байты	2	2	1	3	128	2
Начальный адрес массива A(1)	Первое адресное поле - 0	Второе адресное поле - A(2)	Заголовок кадра – 00100101	Заголо-вок пакета - все 0	Информационная часть пакета – 10 (2)	КПК

…адресная часть … …… кадр ……...

..…. пакет …… ……

байты	2	2	1	3	128	2
Начальный адрес массива А(2)	Первое адресное поле – А(1)	Второе адресное поле - А(3)	Заголовок кадра – 0010111	Заголо-вок пакета - все 0	Информационная часть пакета – 11 (3)	КПК

…адресная часть … …… кадр ……..

..…. пакет ……

байты	2	2	1	3	128	2
Начальный адрес массива А(3)	Первое адресное поле – А(2)	Второе адресное поле - 0	Заголовок кадра – 00101001	Заголо-вок пакета - все 0	Информацион-ная часть пакета – 100 (4)	КПК

…адресная часть … …… кадр ……..

..…. пакет ……

Рис.6. Формат полей MCICL массивов информационных кадров “I” (для контрольного примера (MCICL=3)

$АН_{повт}$

А(1)	А(3)	3

Рис.7. Характеристика $Н_{повт}$

$АН_{п32}$

А(4)	А(8)	5

Рис.8. Характеристика $Н_{п32}$

Лабораторная работа №4

Алгоритм программы приема с канала кадра “REJ”

(см. главы 4,5)

Реализация алгоритма программы приема с канала кадра “REJ” предусматривает последовательное выполнение программы LAB3 (лабораторная работа 3) и программы LAB4, алгоритм которой приводится ниже.

Программа LAB4
Описание:

-константа Z3; исходные данные для 5 вариантов лабораторной работы и контрольного примера приведены в разделе 3.6 лаб. 3 и в разделе 4.5 настоящей лаб. работы.
- переменные D, N(S), N(R), REGIM, CN(R);

- программы DISP4, P_6, P_7, P_8, P_9;

- очереди $O_{кпм}$, $O_{своб.}$

Примечание. Необходимо предусмотреть возможность ввода параметра Z3 перед пуском программы.

Диспетчер программы DISP4

Begin
D := 1

IF D = 1 THEN GO TO P_6 ELSE IF D = 2 THEN GO TO P_7 ELSE

IF D = 3 THEN GO TO P_8 ELSE IF D = 4 THEN GO TO P_9 ELSE

END

Программы:

P_6 – формирование принятого кадра “REJ”, требующего передачу на противоположную сторону кадров “I” с очереди повтора $O_{повт}$;

P_7 – запись этого кадра “REJ”, с контрольно-проверочной комбинацией КПК в первый массив блока очереди $O_{своб.}$ Проверка безошибочного приема кадра REJ с канала связи;

P_8 – перенос кадра REJ (без КПК), поступившего неискаженным, из $О_{своб}$ в очередь принятых с канала кадров $О_{кпм.}$ Установление режима передачи в канал информационного кадра “I” с очереди повтора $О_{повт.}$;

P_9- поставить кадр REJ с начальным адресом массива из очереди принятых с канала кадров $О_{кпм}$ A(N2+1) в конец очереди свободных блоков $О_{своб.}$

По окончании работы программы P_9 необходимо показать результат: содержание в побитовой форме кадра REJ в $О_{кпм}$ перед пересылкой его в очередь $О_{своб.}$

4.1. Программа P_6

Выделение памяти для формирования принятого кадра REJ, требующего передачу с очереди $О_{повт}$ переданных на противоположную сторону кадров “I” (лаб. работа 3). Эта передача должна начинаться с кадра “I” в очереди $О_{повт}$, в заголовке которого N(S) = N(R), где N(R) – параметр принятого кадра REJ. В случае, если в очереди $О_{повт}$ имеются кадры с N(S) < N(R), то они должны быть сняты с $О_{повт}$ и поставлены в очередь свободных блоков $О_{своб.}$ На рис. 1 приведен кадр REJ, включающий байт кадра REJ и 2 байта КПК этого кадра. Начальный адрес этого кадра с КПК - $A(RG_{вх})$. Он имитирует входной регистр с канала $RG_{вх}$, в котором в действительности аппаратным образом проверяется с помощью КПК был ли искажен кадр в канале. $A(RG_{вх})$.

$A(RG_{вх})$

Биты	8	7	6	5	4	3	2	1	16 бит КПК
Значения	0	1	1	0	0	1	0	1	старший байт – все нули младший байт - 01100101

…..N(R)…… …тип кадра…….

……..кадр……

Рис. 1. Формат принятого кадра REJ с КПК во входной регистр с начальным адресом $A(RG_{вх})$

- установить тип кадра REJ: биты кадра <1-4>:= 0101

- установить N(R):=Z3 в биты <6-8> кадра REJ. Это значение N(R) равно значению N(S)= Z3, переданного ранее кадра “I” и находящегося в очереди $О_{повт}$. Параметр Z3 для разных вариантов и контрольного примера приведен в исходных данных (разд. 4.5.). Для

контрольного примера N(S)= Z3=3, т.е. <6-8>:=011 в кадре REJ, что отражено на рис. 1. Это означает, что для контрольного примера в лаб.3 первый и третий кадры “I” соответственно с N(S)=2 и 4 были приняты противоположной стороной правильно, второй кадр был отброшен на приеме из-за искажения в канале (с помощью механизма проверки КПК).

- установить КПК (старший байт равен нулю, младший байт – значение кадра REJ (01100101). Это означает, что кадр REJ принят с канала неискаженным.

D:=D+1
GO TO DISP4

4.2. Программа P_7

Записать в массив по адресу A(N2+1) очереди свободных блоков $O_{своб}$ принятый с канала связи неискаженным кадр REJ (без КПК) (рис.2).

A(N2+1)

Биты	16 бит	16 бит	8	7	6	5	4	3	2	1
Значения	0	0	0	1	1	0	0	1	0	1

….адр. часть…….. ….кадр REJ ……

Рис. 2. Кадр REJ в массиве очереди свободных блоков $O_{своб}$

Откорректировать поля характеристики очереди $H_{своб}$ очереди свободных блоков $O_{своб}$, (т.е. снять свободный блок с начальным адресом массива по A(N2+1) из очереди свободных блоков $O_{своб}$ (рис.3).

$AH_{своб}$

A(N2+2)	A(N1)	N1- N2 -1

Рис.3. Характеристика $H_{своб}$

Установить в ноль первое адресное поле первого массива свободного блока очереди свободных блоков $O_{своб}$ с начальным адресом A(N2+2).

D:=D+1
GO TO DISP4

4.3. Программа P_8

Переписать из очереди свободных блоков $О_{своб}$ кадр REJ (без КПК), поступивший неискаженным, в очередь принятых с канала кадров $О_{кпм.}$(для упрощения рассматривается исходное состояние отсутствия очереди $О_{кпм.}$):

- выделить память под характеристику $Н_{кпм..}$ очереди принятых кадров $О_{кпм..}$ с начальным адресом $АН_{кпм}$;
- установить поля характеристики $Н_{кпм}$ (рис 4);
- поставить в очередь $О_{кпм}$ массив кадра с начальным адресом A(N2+1);

$АН_{кпм}$

A(N2+1)	A(N2+1)	1

Рис.4. Характеристика $Н_{кпм}$

– установление режима передачи в канал информационного кадра “I” с очереди повтора $О_{повт}$ и параметра CN(R), равного N(R) в принятом кадре REJ.

REGIM:=2 (передача в канал кадра “I” ” с очереди повтора $О_{повт.}$)
CN(R):=N(R)

D:=D+1
GO TO DISP4

4.4. Программа P_9

Поставить кадр REJ с начальным адресом массива из очереди принятых с канала кадров $О_{кпм}$ A(N2+1) в конец очереди свободных блоков $О_{своб.}$ Откорректировать поля характеристики очереди $Н_{своб.}$ (рис.5).

$АН_{своб}$

A(N2+2)	A(N2+1)	N2-N1

Рис.5. Характеристика $Н_{своб}$

Установить A(N1) в первое адресное поле и ноль во второе адресное поле в массиве с начальным адресом A(N2+1) очереди свободных блоков $О_{своб.}$

Установить A(N2+1) во второе адресное поле в массиве с начальным адресом A(N1) очереди свободных блоков $О_{своб.}$

Откорректировать поля характеристики очереди $Н_{кпм}$ (рис.6).

$АН_{кпм}$

0	0	0

Рис.6. Характеристика $Н_{кпм}$

D:=D+1
GO TO DISP4

4.5. Исходные данные для лабораторной работы

В таблице 1 приведены исходные данные пяти вариантов лабораторной работы и контрольного примера.

Таблица 1. Исходные данные для лабораторной работы

Параметр	1 вариант	2 вариант	3 вариант	4 вариант	5 вариант	Контрольный вариант
Z3	2	3	3	4	5	3

Некоторые характеристики контрольного примера

$АН_{своб}$

A(10)	A(20)	11

Рис.3. Характеристика $Н_{своб}$

$АН_{кпм}$

A(9)	9	1

Рис.4. Характеристика $Н_{кпм}$

$АН_{своб}$

A(10)	A(9)	12

Рис.5. Характеристика $Н_{своб}$

Лабораторная работа №5

Алгоритм программы передачи в канал кадров “I” с очереди повтора $О_{повт}$

Реализация алгоритма программы LAB5 предусматривает последовательное выполнение программы LAB3 (лабораторная работа 3), программы LAB4 (лабораторная работа 4) и программы LAB5, алгоритм которой приводится ниже.

Программа LAB5
Описание:

-константы; исходные данные для 5 вариантов лабораторной работы и контрольного примера приведены в разделе 3.6 лаб. 3 и в разделе 4.5 лаб. 4.

- переменные D,TADR, K, REGIM, CN(R);
- программы DISP5, P_{10}, P_{11}, P_{12};
- очереди $О_{повт}$, $О_{своб.}$

Begin

REGIM:=2 (передача в канал кадра “I” ” с очереди повтора $О_{повт.}$)

IF MCICL > 0 THEN TADR:= $АН_{повт}$ (первое адресное поле) END ELSE OSHIBKA END; т.к. в очереди $О_{повт.}$ есть кадры “I”, то в значение текущего адреса TADR устанавливается по первому полю характеристики $Н_{повт}$ начальный адрес массива первого кадра в $О_{повт.}$, т.е. A(1). Это значение и значение MCICL берутся из характеристики очереди $О_{повт.}$ (см. рис. 7, лаб. работа 3).

K:=1
END

Диспетчер программы DISP5

Begin
D := 1
IF D = 1 THEN GO TO P_{10} ELSE IF D = 2 THEN GO TO P_{11} ELSE

IF D = 3 THEN GO TO P_{12} ELSE

END

Программы:

P_{10} – программа проверки необходимости стирания и повторной передачи кадров “I” с очереди повтора $О_{повт.}$

$Р_{11}$ – программа стирания кадра (кадров) “I” с очереди повтора $О_{повт.}$

$Р_{12}$ – программа передачи в канал кадров “I” с очереди повтора $О_{повт.}$

По окончании работы программы $Р_{12}$ по исходным данным необходимо показать результат:

- содержание в побитовой и десятичной форме полей кадра в очереди $О_{повт}$ перед тем, как он будет перенесен в очередь $О_{своб}$ и станет там последним (после завершения работы всей программы $Р_{12}$);
- содержание полей в побитовой и десятичной форме всех находящихся в $О_{повт}$ информационных кадров.

Примечание. Под содержанием полей кадра имеется в виду N(S), N(R) и тип кадра в его заголовке, а также информационная часть входящего в него пакета.

5.1. Программа $Р_{10}$

Сравнить N(S) массива кадра “I” в очереди $О_{повт}$ по начальному адресу TADR с параметром CN(R), равным N(R) принятого ранее кадра REG.. Значение N(S)= биты заголовка <2-4> этого кадра (программа $Р_{3,}$ лаб.3). Значение параметра CN(R) – (программа $Р_{8,}$ лаб.4).

IF N(S)< CN(R) THEN D:=2 ELSE D:=3
GO TO DISP5 END; при D:=2 – перенос кадра в $О_{своб,}$ при D:=3 - передача в канал кадров “I” с очереди повтора $О_{повт..}$

5.2. Программа $Р_{11}$

Перенести массив первого кадра “I” по начальному адресу TADR из очереди $О_{повт}$ в очередь свободных блоков $О_{своб.}$

Откорректировать характеристику очереди повтора $О_{повт}$, т.е. $Н_{повт}$ (рис.1).

$АН_{повт}$

Второе адресное поле TADR	A(MCICL)	MCICL-K

Рис.1. Характеристика $Н_{повт}$
Первое поле $Н_{повт}$:=второе поле массива по начальному адресу TADR (т.е. A(2) для контрольного примера лаб. 3).

Установить в ноль первое адресное поле массива кадра с начальным адресом первого поля $Н_{повт.}$

Откорректировать характеристику очереди свободных блоков $Н_{своб.}$ (рис.2).

$АН_{своб}$

A(N2+1)	TADR	N1- N2+ К

Рис.2. Характеристика $Н_{своб}$

Установить в ноль второе адресное поле массива кадра с начальным адресом TADR т.е. A(1) для контрольного примера и значение A(N1) в его первое адресное слово.

Установить TADR A(1) во второе адресное слово массива кадра с начальным адресом TADR A(N1). Очистить информационные поля этого массива кадра очереди свободных блоков $О_{своб}$.

TADR:= TADR (второе адресное поле).

К:=К+1
D:= 1
GO TO DISP5

5.3. Программа $Р_{12}$

Скопировать кадр “I” из массива этого кадра с начальным адресом TADR в
в выходной регистр передачи $RG_{вых}$ в канал связи. Передать в канал этот кадр из регистра $RG_{вых.}$ Очистить регистр $RG_{вых.}$

IF К= MCICL (последний кадр в $О_{повт}$) THEN D:= 4 ELSE

установить в значение текущего адреса TADR начальный адрес массива следующего кадра в $О_{повт.}$, TADR:= TADR (второе адресное поле).

К:=К+1
D := 1
GO TO DISP5

5.5. Некоторые характеристики контрольного примера

$АН_{повт}$

A(2)	A(3)	2

Рис.1. Характеристика $Н_{повт}$

$АН_{своб}$

A(9)	A(1)	13

Рис.2. Характеристика $Н_{своб}$

Лабораторная работа №6

Алгоритм программы приема информационного кадра “I”

(см. главы 4,5,6,7)

Реализация алгоритма программы приема с канала кадра “I” предусматривает последовательное выполнение программы LAB3 (лабораторная работа 3) и программы LAB6, алгоритм которой приводится ниже.

Программа LAB6

Описание:

- константы N1, N2, Z2, *m*, Y;
- переменные D, V(R), N1(R), N(S), i, j,TADR;
- программы DISP6, P_6, P_7, P_8, P_9, P_{10};
- очереди $O_{кпм}$, $O_{своб}$, $O_{повт}$, $O_{п23}(j)$.

Диспетчер программы DISP6

Begin;

D:= 1

IF D = 1 THEN GO TO P_6 ELSE IF D = 2 THEN GO TO P_7 ELSE

IF D= 3 THEN GO TO P_8 ELSE IF D = 4 THEN GO TO P_9 ELSE

IF D = 5 THEN GO TO P_{10} ELSE

END

P_6 – формирование принятого кадра “I”, подтверждающего правильный прием первого из всех переданных на противоположную сторону информационных кадров “I” (см. лаб. 3);

P_7 – Программа записи кадра “I” с контрольно-проверочной комбинацией КПК в первый блок очереди $O_{своб}$;

P_8 – программа переноса принятого кадра “I” из $O_{своб}$ в очередь $O_{кпм}$;

P_9 – программа считывания правильно принятых противоположной стороной ранее кадров “I” и находящихся в очереди повтора $O_{повт}$ (лаб.3);

P_{10} – программа: 1) перепись пакета принятого кадра “I” (находящегося в очереди $O_{кпм}$) в очередь на передачу с канального процессора j=5 $O_{п23}(j)$ в центральный процессор сетевого

уровня (рис. 7.2 лекция 7); 2) передача пакета в $О_{п23}(5)$ в регистр передачи на сетевой уровень REG_{23}.

По окончании работы программы $Р_{10}$ по исходным данным необходимо показать результат:

- содержание в побитовой и десятичной форме информационного поля пакета (заголовок пакета - 0) в регистре передачи на сетевой уровень REG_{23};
- содержание в побитовой и десятичной форме полей кадра в очереди $О_{повт}$ перед тем, как он будет перенесен программы $Р_9$ в очередь $О_{своб}$ и станет там последним;
- содержание в побитовой и десятичной форме полей кадров в очереди $О_{повт}$ (после завершении работы программы $Р_9$.

Примечание. Под содержанием полей кадра имеется в виду N(S), N(R) и тип кадра в его заголовке, а также информационная часть входящего в него пакета.

6.1. Программа $Р_6$

Выделение памяти для формирования принятого информационного кадра “I”, подтверждающего правильный прием всех переданных на противоположную сторону информационных кадров “I” (лаб. 3).

На рис.1 приведен этот формат этого кадра, включающий 1 байт заголовка кадра, 2 байта заголовка пакета, 128 байт информационной части пакета и 2 байта КПК этого кадра. Начальный адрес этого кадра с КПК - $А(RG_{вх})$. Он имитирует входной регистр $RG_{вх}$ с канала, в котором в действительности аппаратным образом проверяется с помощью КПК был ли искажен кадр в канале. Как видно из рис.1 регистр состоит из 133-х байтов.

байты	1	2	128	2
начальный адрес $А(RG_{вх})$	Заголо-вок кадра	Заголо-вок пакета	Информационная часть пакета	КПК

…… кадр ……..

…….. ……..……. пакет ……..

Рис.1. Формат принятого информационного кадра “I” во входной регистр с начальным адресом $А(RG_{вх})$

Сформировать поля принятого кадра (значения приведены для контрольного примера):

- записать данные m+5 в поле информационной части пакета (для контрольного примера m+5=6, т.е. 110).

- установить ноль в поле заголовка пакета.

Установить параметры заголовка принятого кадра (значения приведены для контрольного примера):

- установить тип кадра “I”: биты кадра <1>:= 0

- установить V1(S):=Z2; переменный параметр очередного информационного кадра “I” на передачу с противоположной стороны (т.е. N1(S) принятого кадра совпадает с ожидаемым)

- установить N1(S):= V1(S) и записать в биты принятого кадра <2-4>:=001

- установить V1(S) := V1(S) +1

- установить N1(R):=V1(R) в биты кадра <6-8>:=100; в программе лаб.3 в контрольном примере на противоположную сторону были отправлены три “I” кадра соответственно с N(S) (битами в заголовке <6-8>:= 010, 011, 100). Биты принятого кадра с N1(R) <6-8>:=100 показывают, что приняты правильно первые два из них (ожидается на противоположной стороне “I” кадр с N(S) = 100.

- установить КПК (старший байт равен нулю, младший байт – 10000100, т.е. суммированные по модулю 2 все байты кадра (10000010 – заголовок кадра, информационная часть пакета - 110). Это означает, что кадр принят неискаженным в канале.

D:=D+1
GO TO DISP6

6.2. Программа P_7

Записать в массив первого блока по адресу A(N2+1) очереди свободных блоков $O_{своб}$ принятый с канала связи кадр “I”, подтверждающий правильный прием с противоположной стороны двух (из трех переданных) информационных кадров “I” (рис.2). Значения полей заголовка принятого кадра приведены для контрольного примера.

A(N2+1)

Биты	16 бит	16 бит	8	7	6	5	4	3	2	1
Значения	0	0	1	0	0	0	0	0	1	0

….адр. часть…… ….кадр “I” ……..

Рис. 2. Заголовок кадра “I” в массиве очереди свободных блоков $О_{своб}$

- откорректировать поля характеристики очереди $Н_{своб}$ очереди свободных блоков $О_{своб}$, (т.е. снять свободный блок с начальным адресом массива по A(N2+1) из очереди свободных блоков $О_{своб}$ (рис.3).

$АН_{своб}$

A(N2+2)	A(N1)	N1- N2 -1

Рис.3. Характеристика $Н_{своб}$

- установить в ноль первое адресное поле первого массива свободного блока очереди свободных блоков $О_{своб}$ с начальным адресом A(N2+2).

D:=D+1
GO TO DISP6

6.3. Программа $Р_8$

Переписать из очереди свободных блоков $О_{своб}$ кадр “I” (без КПК), поступивший неискаженным, в очередь принятых с канала кадров $О_{кпм}$ (для упрощения рассматривается исходное состояние отсутствия очереди $О_{кпм.}$):

- выделить память под характеристику $Н_{кпм.}$ очереди принятых кадров $О_{кпм.}$ с начальным адресом $АН_{кпм}$;
- установить поля характеристики $Н_{кпм}$ (рис 3);
- поставить в очередь $О_{кпм}$ массив кадра с начальным адресом A(N2+1);

$АН_{кпм}$

A(N2+1)	A(N2+1)	1

Рис.4. Характеристика $Н_{кпм}$

- установить значение ноль в оба адресные поля массива кадра с начальным адресом A(N2+1);

- проверить есть ли в $О_{повт}$ кадры, на которые пришла квитанция об их правильном приеме.

Определить N(S) первого кадра в $О_{повт}$: по первому полю $Н_{повт}$ определяем адрес массива первого кадра в $О_{повт}$; N(S):= биты <2-4> заголовка этого кадра. Для контрольного примера рис.7 лаб.3 N(S)=010. N1(R) - <6-8> принятого кадра “I” и находящегося в очереди $О_{кпм.}$ Для контрольного примера N1(R) = 100.

IF N(S) =< N1(R)-1 THEN
D:=D+1
GO TO DISP6
ELSE END

6.4. Программа $Р_9$

Y:= N1(R) - N(S) ; число кадров, на которые пришла квитанция об их правильном приеме.

Установить TADR := <первое поле> характеристики $Н_{повт,}$ т.е. адрес массива первого кадра в $О_{повт.}$

FOR i = 1 ... Y DO
Поставить массив кадра по адресу TADR из очереди $О_{повт}$ в очередь $О_{своб}$
IF i = Y THEN
Откорректировать $О_{повт}$ и $О_{своб}$, $Н_{повт}$ и $Н_{своб.}$
END ELSE

В первое поле характеристики $Н_{повт}$ записать второе адресное слово массива кадра по адресу TADR из очереди $О_{повт.}$

В третьем поле $Н_{повт}$ значение уменьшить на единицу.

Второе адресное слово массива по адресу TADR записать в первое поле характеристики $Н_{повт,}$ а в третьем поле $Н_{повт}$ значение уменьшить на единицу.

В первое адресное поле массива по адресу TADR записать второе адресное поле массива второго поля характеристики $Н_{своб.}$ Во второе адресное поле TADR записать ноль.

Во второе адресное поле массива второго поля характеристики $Н_{своб}$ записать TADR. . Во второе поле $Н_{своб}$ записать TADR, а в третьем поле $Н_{своб}$ прибавить единицу.

TADR:= <первое поле> $Н_{повт}$
END

На рис. 5 приведена характеристика очереди $Н_{повт}$ (очереди $О_{повт}$) при исходных данных контрольного примера.

$АН_{повт}$

A(3)	A(3)	1

Рис.5. Характеристика $Н_{повт}$

На рис. 6 приведена характеристика очереди $Н_{своб}$ (очереди свободных блоков $О_{своб}$) при исходных данных контрольного примера.

$АН_{своб}$

A(N2+2)	A(2)	N1- N2 +1

Рис.6. Характеристика $Н_{своб}$

D:=D+1
GO TO DISP6

6.5. Программа $Р_{10}$

Выполнить следующую последовательность операций.

Переписать пакет принятого кадра “I” (находящегося в очереди $О_{кпм}$) в очередь на передачу с канального процессора j=5 $О_{п23}(j)$ в центральный процессор сетевого уровня (рис. 7.2 лекция 7).

Переслать этот из $О_{п23}(5)$ в регистр передачи на сетевой уровень REG_{23}.

Перенести в конец $О_{п23}(5)$ массив принятого кадра “I” по адресу A(N2+1) и находящегося в очереди $О_{кпм}$.

Убрать заголовок кадра, оставив входящий в него пакет.

На рис.7 приведен формат массива этого пакета без указания содержания заголовка и информационной части.

байты	2	128

начальный адрес $A(RG_{вх})$	Заголо-вок пакета	Информационная часть пакета

… . ..…… пакет ……

Рис.7. Формат массива пакета в принятом информационном кадре “I”

Откорректировать очереди $O_{кпм}$, $O_{п23}(5)$ и характеристики этих очередей $H_{кпм}$, $H_{п23}(5)$
Передача этот пакет в $O_{п23}(5)$ в регистр передачи на сетевой уровень REG_{23} и перенести массив этого пакета в конец $O_{своб.}$
-Откорректировать очереди $O_{п23}(5)$, $O_{своб}$ и характеристики этих очередей $H_{п23}(5)$, $H_{своб.}$
На рис. 8 приведена характеристика очереди $H_{своб}$ (очереди свободных блоков $O_{своб}$) при исходных данных контрольного примера.

$AH_{своб}$

A(N2+2)	A(N2+1)	N1- N2 + 2

Рис.8. Характеристика $H_{своб}$

D:=D+1
GO TO DISP6

6.6. Исходные данные для лабораторной работы

В таблице 1 приведены исходные данные пяти вариантов лабораторной работы и контрольного примера.

Таблица 1. Исходные данные для лабораторной работы

Параметр	1 вариант	2 вариант	3 вариант	4 вариант	5 вариант	Контрольный вариант
N1	15	14	13	12	11	20

N2	7	7	7	7	7	8
Z2	0	3	2	4	5	1
m	2	3	4	5	6	1

Некоторые характеристики контрольного примера

$АН_{своб}$

A(10)	A(20)	11

Рис.3. Характеристика $Н_{своб}$

$АН_{кпм}$

A(9)	A(9)	1

Рис.4. Характеристика $Н_{кпм}$

$АН_{своб}$

A(10)	A(2)	13

Рис.6. Характеристика $Н_{своб}$

$АН_{своб}$

A(10)	A(9)	14

Рис.8. Характеристика $Н_{своб}$

ГЛАВА 6. Информационные процессы на сетевом уровне сети X.25

6.1. Принцип установления виртуальных каналов в сети X.25

Третий (сетевой) уровень выполняет функцию коммутации пакетов сети передачи данных стандарта МСЭ-Т X.25. Описание принципа коммутации пакетов приведено в главе 2. Сетевой уровень X.25 соответствует функции третьего уровня эталонной модели OSI – коммутация (маршрутизация) блока данных (в случае X.25 – пакета данных “Д”). На сетевом уровне протокол X.25/3 обеспечивает для уровней, расположенных выше в иерархии сервис с установлением соединений. Поэтому на этом уровне определены процедуры установления виртуальных соединений, передачи данных по виртуальным соединениям и разрыва виртуальных соединений. При использовании сервиса, ориентированного на соединение, каждый пакет данных вместо физического адреса включает в свой заголовок виртуального канала уникальный на узле коммутации номер, соответствующий логическому каналу. Протокол виртуального соединения стандарта X.25 является мультиплексируемым протоколом, т.е. через один канал связи второго уровня может быть установлено много виртуальных соединений. Виртуальные соединения отличаются друг от друга уникальными *логическими канальными номерами* (LCN – *Logical Channel Number*). В качестве примера покажем передачу по одному и тому же каналу второго уровня пакетов двух разных виртуальных соединений (рис. 6.1).

На рис. 6.1 показана маршрутизация двух виртуальных соединений (каналов): одного между оконечными станциями Н1- Н2, другого между оконечными станциями Н3 – Н4. *Центр коммутации пакетов* X.25 ЦКП(А) может отличить пакеты, поступающие от Н1 и Н3 (номера LCN у них одинаковые и равны 1), так как эти пакеты поступают в ЦКП(А) по разным физическим линиям. Следующий за ним ЦКП(С) различить эти пакеты не может. Поэтому, для того, чтобы различить виртуальные соединения Н3 - Н4 и Н1 - Н2 в заголовке пакета первого соединения устанавливается уникальное для этого центра LCN, а в заголовке пакета второго соединения другое уникальное LCN, На рис 6.1 эти значения равны соответственно 19 и 144. Эти пакеты поступают на основании физических адресов оконечных станций в соответствии с таблицей маршрутизации в ЦКП(С). В ЦКП(С) на выходе в заголовке пакета первого соединения устанавливается уникальное для этого центра LCN(73), а в заголовке пакета второго виртуального соединения другое уникальное LCN(75). Аналогичная процедура выполняется в последнем ЦКП(Е). Таким образом, на одних и тех же участках сети ЦКП(А)-ЦКП(С)-ЦКП(Е) передаются пакеты двух разных виртуальных

каналов (ВК).

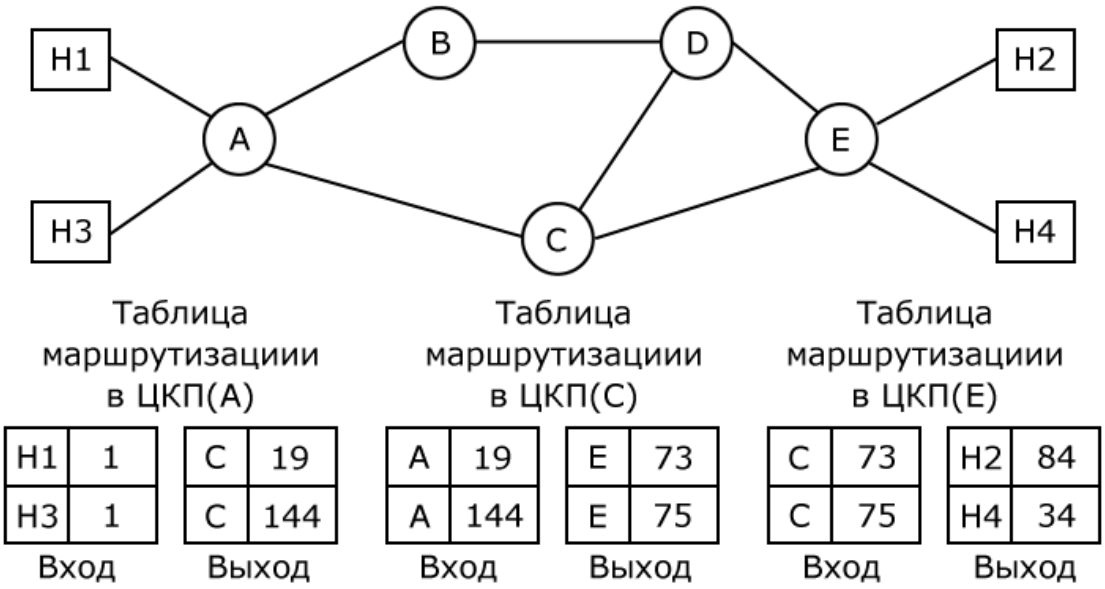


Рис. 6.1. Пример виртуальных соединений по одному каналу второго уровня

Сеть X.25 обеспечивает два вида сервиса установления соединения: *постоянный виртуальный канал* ПВК (PVC – *Permanent Virtual Circuit*) и *коммутируемый виртуальный канал* КВК (SVC – *Switched Virtual Circuit*).

Логические канальные номера LCN в таблицах маршрутизации ПВК устанавливаются оператором сети, т.е. отсутствует обмен служебными пакетами по установлению виртуального канала. Необходимость в таких каналах возникает у пользователей, которые нуждаются в постоянном соединении между ними. При большой интенсивности потоков предпочтительно использовать ПВК, который является более дешевой альтернативой арендованному каналу.

Основным недостатком ПВК является его низкая надежность, так как сеть не позволяет быстро и безошибочно восстановить соединение между пользователями при неисправности звена данных (канала связи) между ЦКП. КВК устанавливается автоматически с помощью служебных пакетов. Описание установления КВК приводится позже.

Режим коммутируемого виртуального канала КВК используется в тех случаях, когда информация передается между многими пользователями, а сеансы связи не частые или кратковременные. Применение в этих случаях ПВК означало бы установление соединений между всеми пользователями и необходимость производить оплату бездействующих соединений. Мультиплексирование в режиме КВК позволяет экономично использовать пропускную способность каналов связи и выгодно для пользователей сети.

На рис. 6.2 приведена иллюстрация мультиплексирования нескольких виртуальных каналов в один канал связи между ЦКП. Здесь через ВК1 обозначен виртуальный канал, соединяющий абонентов 1 и 1*, через ВК2 обозначен виртуальный канал, соединяющий абонентов 2 и 2*, через ВК3 обозначен виртуальный канал, соединяющий абонентов 3 и 3*, через ВК4 обозначен виртуальный канал, соединяющий абонентов 4 и 4*. На участке между ЦКП4 и ЦКП5 проходят все эти виртуальные каналы.

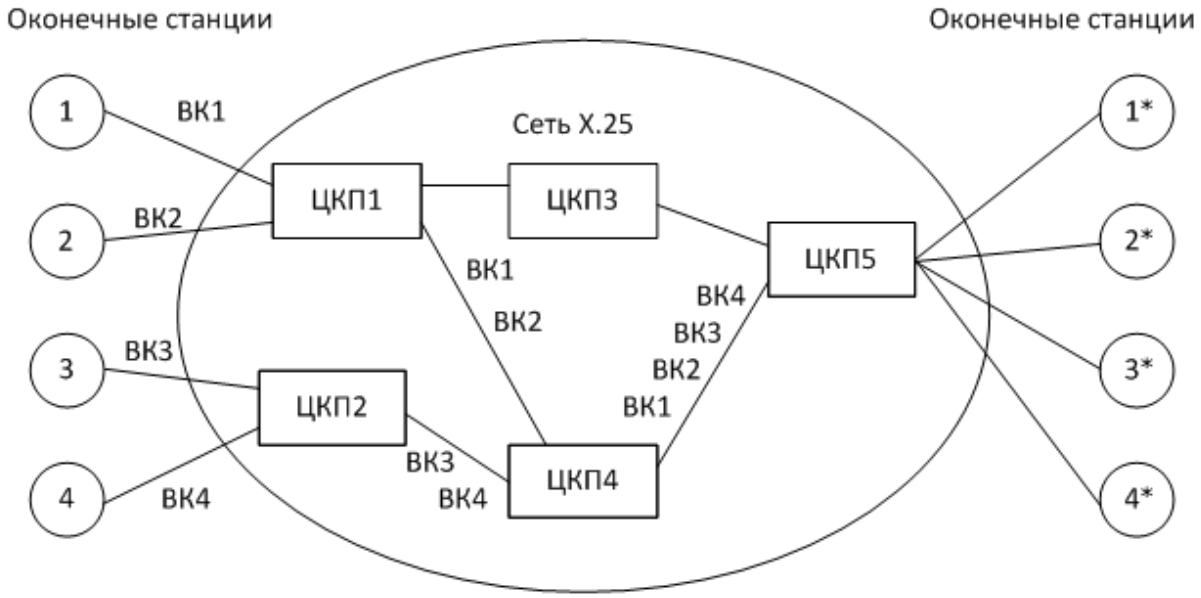


Рис. 6.2. Мультиплексирование виртуальных каналов

На рис. 6.3 приведены два виртуальных канала (КВК или ПВК), проходящие через три ЦКП. В первом виртуальном канале (КВК1 или ПВК1), изображенном сплошными линиями:

- логический канальный номер LCN в заголовке входящего пакета в ЦКП1 –равен 5, в заголовке исходящего пакета – 3503;
- в ЦКП2 соответственно 3503 и 1510;
- в ЦКП3 соответственно 1510 и 2301.

Во втором виртуальном канале (изображенном пунктирными линиями):

в ЦКП1 - 2020 и 1500; в ЦКП2 - 1500 и 835; в ЦКП3 - 835 и 4001.

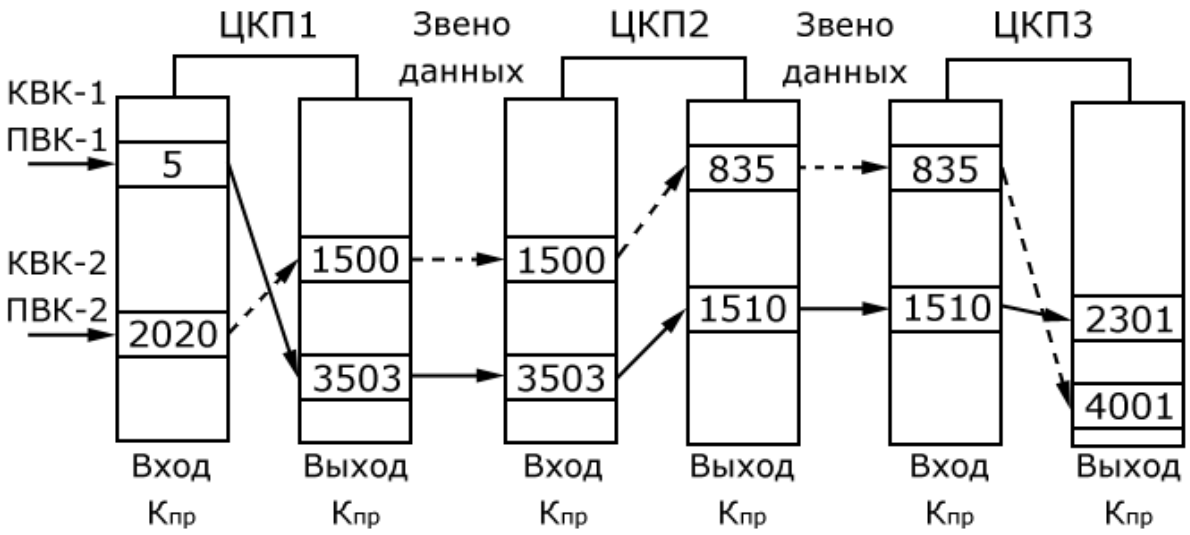


Рис. 6.3. Прохождение пакетов двух виртуальных каналов через несколько ЦКП

Для того чтобы обеспечить индивидуальность виртуального канала, номер LCN в заголовке исходящего из ЦКП пакета должен быть уникальным. Это обеспечивается программным способом при установлении ВК с использованием свободного номера, не задействованного в этом ЦКП никаким другим соединением.

Рассмотрим информационные процессы в *коммутируемом виртуальном канале*. На рис. 6.4 приведен пример сети X.25 с вычислительными средствами ЦКП1 и ЦКП2. Каждый из этих ЦКП состоит из центрального процессора (Цпр), выполняющего функции сетевого уровня и канальных процессоров, выполняющих функции канального уровня (Кпр).

Как видно из рисунка, канальные процессоры Кпр1, Кпр2, Кпр3 ЦКП1 и ЦКП2 взаимодействуют с центральным процессором Цпр своего ЦКП и процессорами оконечных станций (Пр). Канальные процессоры Кпр4, Кпр5, Кпр6 взаимодействуют с центральным процессором Цпр своего ЦКП и канальными процессорами смежных ЦКП.

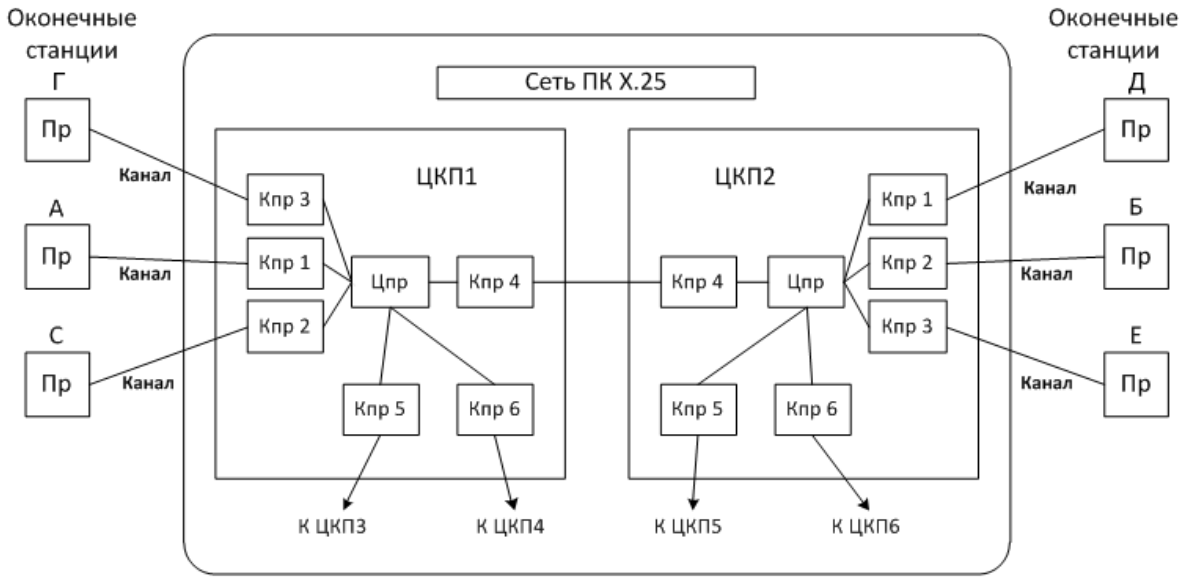


Рис. 6.4. Вычислительные средства двух ЦКП сети X.25
Процессоры оконечных пунктов выполняют функции всех уровней модели OSI.

6.2. Диаграмма установления коммутируемого виртуального канала

На рис. 6.5 приведена упрощенная диаграмма установления КВК между оконечными пунктами А и Б и передача пакета данных «Д» по этому КВК от А в Б. Обработка пакетов «Запрос Вызова» и «Вызов Принят» выполняет одновременно функции составления таблицы маршрутизации по логическим канальным номерам LCN и установление коммутируемого виртуального канала.

Приведем краткое описание этих информационных процессов:

- с транспортного уровня оконечной станции А на сетевой уровень поступает примитив «Запрос» на установление КВК между А и Б;
- с сетевого уровня на канальный уровень станции А поступает пакет «Запрос вызова» («ЗВ»), в заголовке которого размещены физические адреса оконечных станций А и Б (адресация по рекомендации X.121) и логический канальный номер LCN=1. Адреса X.121 имеют максимальную длину, равную 14 цифрам, из которых одна цифра — код зоны. МСЭ-Т разделил мир на 7 зон, три цифры — идентификатор сети в зоне, десять цифр — номер сетевого терминала;
- с канального уровня станции А в ЦКП1 поступает кадр «I» с вложенным (инкапсулированным) в него пакетом «ЗВ». Кадр передается в канал связи;

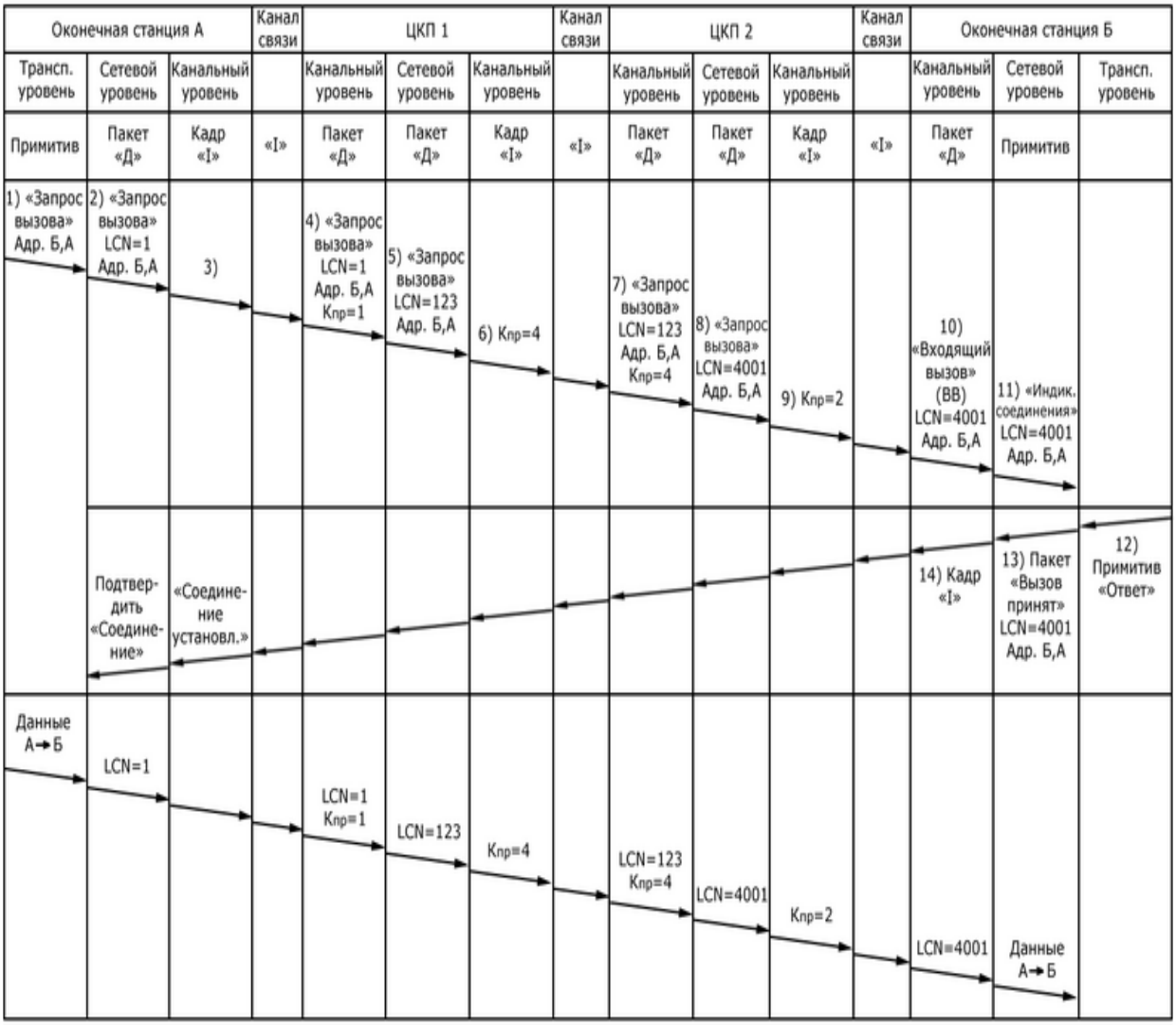


Рис. 6.5. Установление КВК и передача по нему пакета данных

- кадр «I» с входящим в него пакетом «3В» поступает на канальный процессор Кпр1 ЦКП1; На выходе Кпр1 этот кадр освобождается от заголовка и вложенный в него пакет «3В» поступает на центральный процессор Цпр.
- центральный процессор Цпр выполняет функции сетевого уровня и производит коммутацию этого пакета на Кпр4, установив при этом в заголовке новое значение LCN=123. Коммутация производится с помощью таблицы маршрутизации на основании физических адресов А и Б в заголовке пакета;
- кадр «I» с пакетом «3В» (с заголовком LCN=123) поступает на Кпр4 ЦКП2. На выходе Кпр4 кадр освобождается от заголовка;
- пакет с LCN=123 в заголовке поступает на Цпр ЦКП2, где производится его коммутация на Кпр2 и установка нового значения LCN=4001;

- на выходе Кпр2 ЦКП2 формируется кадр «I» с вложенным в него пакетом «ЗВ» (LCN=4001);
- этот кадр передается в канал и затем поступает на процессор оконечной станции Б;
- на оконечной станции Б кадр освобождается от заголовка после его обработки, и входящий в него пакет под измененным названием («Входящий вызов» – «ВВ») с LCN = 4001 поступает на сетевой уровень;
- после обработки заголовка поступившего пакета «ВВ» Цпр оконечной станции Б направляет примитив «индикация соединения» на транспортный уровень с указанием адресов А и Б;
- с транспортного уровня поступает примитив «ответ»;
- при положительном решении сетевой уровень оконечной станции Б формирует пакет «Вызов принят» («ВП») с LCN = 4001;
- Цпр отправляет «I» кадр с вложенным в него пакетом «ВП».

Далее в обратном направлении по тому же пути до оконечной станции А пересылается информационный кадр, и на сетевой уровень А поступает пакет под названием «Соединение установлено» с LCN = 1. С сетевого уровня на транспортный уровень поступает примитив «подтверждение соединения». На этом завершается фаза установления КВК между оконечными пунктами А и Б. Следующая строка на диаграмме иллюстрирует прохождение от А в Б пакета «Данные» («Д») по установленному КВК.

Примитив с транспортного уровня сообщает сетевому уровню о необходимости передачи пакета «Д» по КВК между А и Б. Сетевой уровень пункта А формирует пакет «Д» с LCN = 1. Физические адреса А и Б в пакетах с данными «Д» отсутствуют, так как все пакеты с данными, принадлежащие информационному потоку А Б, будут пересылаться через сеть по одному и тому же маршруту, установленному КВК. Как видно из диаграммы, пакет «Д» проходит через ЦКП1 и ЦКП2 в оконечный пункт Б по тому же маршруту (через те же канальные процессоры) и с теми же логическими канальными номерами LCN, которые были во входящем и исходящем пакетах «Запрос вызова» и «Вызов принят».

В обратном направлении пакет «Д» (из Б в А) будет проходить по тому же маршруту и логические канальные номера LCN будут устанавливаться, как в выше приведенных пакетах «Вызов принят» и «Соединение установлено».

Установление КВК и передача пакетов «Д» между другими оконечными пунктами, подключенными к ЦКП1 и ЦКП2 (например, С-Д, Г-Е) производится через соответствующие

канальные процессоры абонентского доступа (С - через Кпр2 ЦКП1, Г - через Кпр3 ЦКП1), но через одни и те же канальные процессоры Кпр4, подключенные к каналу связи между ЦКП1 и ЦКП2.

Логические канальные номера LCN в пакетах, передаваемых между ЦКП1 и ЦКП2, должны быть индивидуальными для каждого КВК. На этом участке могут проходить пакеты «Д» по всем КВК, максимальное число которых определяется в X.25 полем в 12 бит. Максимальное число виртуальных каналов, обслуживаемых центральным процессором одного ЦКП, составляет 4094.

Перечислим некоторые из основных полей заголовка пакета сетевого уровня X.25:

- *логический канальный номер* LCN;
- *тип пакета* (пакеты установления и сброса виртуального соединения, пакеты данных «Д» верхних уровней, пакеты управления потоком, пакеты прерываний, пакеты подтверждения прерываний). Длина поля данных пользователя в пакете дана по умолчанию равной 128 байт, но доступны также и другие значения: 16, 32, 64, 256, 512, 1024, 2048 и 4096 байт;
- *биты специальных операций* (D – бит, M – бит, Q – бит).

Пакеты прерываний обеспечивают механизм, при помощи которого могут быть отправлены срочные данные. Большинство производителей оборудования поддерживают две очереди пакетов «Д» для каждого выходного порта – одна для обычных данных, а другая для данных прерываний (т.е. с приоритетом). Прежде чем обслуживать обычную очередь производится проверка того, что очередь пакетов прерываний пуста.

Управление потоком данных является важным аспектом сервиса X25/3 по причине природы операций виртуального соединения, требующих гарантированной доставки данных. Для гарантии того, что пакеты не потеряются, важно ограничить количество неподтвержденных пакетов, т.е. размер окна виртуального канала сетевого протокола.

На сетевом уровне X25/3 предусмотрена возможность остановить отправку пакетов «Д» при получении пакета RNR - receive not ready (*неготовность к приему*) по определенному виртуальному каналу. Этот механизм используется для снятия перегрузки.

6.3. Особенности протокола сетевого уровня X.25

При сравнении с сетевым уровнем модели OSI других технологий сетей протокол сетевого уровня X25/3 имеет несколько отличий. Этот стандарт не содержит *протокола*

маршрутизации. Под протоколом маршрутизации понимается автоматическая коррекция таблиц маршрутизации при отказах каналов связи, перегрузке и других изменениях в сети. Эти функции в сети X.25 (относительно таблицы маршрутизации по физическим адресам) отнесены к специфике реализации. Следует отметить, что протоколы маршрутизации разработаны в стандартах других сетей связи, (например, в системе сигнализации ОКС№7, в IP-сети). Эти протоколы учитывают коррекцию таблицы маршрутизации при отказах каналов связи и узлов коммутации, при перегрузках.

X.25 является *протоколом интерфейса абонентского доступа*.

На абонентском доступе сети X.25 располагается два вида оборудования:

- *оконечное оборудование данных* ООД (DTE, *Data Terminal Equipment*), машина конечного пользователя, в качестве которой может быть терминал или компьютер;
- *оборудование окончания канала данных* АКД (DCE, *Data Circuit-terminating Equipment*). Функция канала данных состоит в подключении ООД к каналу передачи данных. АКД преобразует цифровой сигнал ООД в сигналы, согласованные с характеристиками существующих каналов связи (аналоговых или цифровых). Примером АКД является модем.

Протокол сетевого уровня X25/3 выполняет несколько функций, которые обычно относятся к функциям транспортного уровня. Операции включают использование нескольких специальных битов в заголовках пакетов. Пакеты данных X.25 содержит D – бит, Q – бит и M – бит.

Сквозное подтверждение (D – бит)

Когда бит D установлен в 1, то предусмотрено сквозное подтверждение приема пакета, т.е. от одного *оконечного оборудования данных* (ООД) до другого ООД. Если пакет с D=1 достигает ООД получателя, то это оборудование отвечает за обеспечение подтверждения. Это подтверждение направляется обратно к ООД отправителя, таким образом, реализуя сквозное подтверждение. В этом случае с транспортного уровня снимается функция гарантии правильной последовательности принятых пакетов, которая обычно имеет место в сетях других технологий.

В сети X.25 в большинстве случаев используется локальное подтверждение правильного приема пакетов, т.е. на участке между ООД и аппаратурой канала данных АКД. В этом

случае за проверку правильной последовательности пакетов во входящем потоке отвечает транспортный уровень (четвертый уровень OSI).

Формирование и сборка пакетов данных (M – бит)

В соответствии с моделью OSI, транспортный уровень отвечает за сегментацию сообщений таким образом, чтобы размер сегмента не превышал максимального размера пакета, требуемого сетевым уровнем. Транспортный уровень получателя выполняет процесс обратный сегментации, чтобы восстановить сообщение. Посредством M – бита в заголовке пакета «Д» протокол сетевого уровня X25/3 забирает у транспортного уровня функцию сегментации сообщений и их сборки. Результатом является последовательность связанных пакетов, которые после сборки образуют исходное сообщение. Для этого отправитель устанавливает M – бит всех пакетов за исключением последнего в последовательности пакетов в 1. В последнем пакете последовательности M – бит устанавливается в 0. На основании значений M – бита, получатель может собрать пакеты в исходное сообщение, прежде чем оно будет передано на транспортный уровень.

Отправка данных специального назначения (Q – бит)

Q – бит, находящийся в заголовке пакета данных, используется для указания альтернативного места назначения для содержимого поля пользовательских данных определенного пакета. В обычных условиях Q – бит в пакете «Д» установлен в 0. Это значит, что содержащиеся в пакете данные предназначены для конечного пользователя. Если Q – бит установлен в 1, это значит, что получатель содержимого поля является не «типичным» конечным пользователем, а некоторым другим объектом в местоположении получателя. Например, можно управлять конфигурацией удаленного конечного пользовательского устройства во время установленного виртуального соединения. Допустим, мы хотим изменить значение параметра канального уровня (такого как размер окна) во время обмена пакетами «Д». Для этого, используя Q - бит, можно отправить команду с новыми параметрами настройки в поле данных пакета X.25. Когда этот пакет достигнет получателя, его содержимое будет направлено не на сетевой уровень, а на канальный уровень. Таким образом, Q – бит позволяет выбрать одно их двух мест назначения для содержимого каждого пакета «Д». Так как Q – бит занимает поле в 1 бит, то поддерживается один «нетипичный» конечный пользователь, который определяется во время установления соединения.

6.4. Услуга информационной безопасности «Замкнутая группа абонентов»

В рекомендации X.25 предусмотрены дополнительные услуги. Замкнутая группа

пользователей CUG (*Closed User Group*) является одной из таких услуг и служит средством обеспечения безопасности в отношении защиты от несанкционированного доступа. Членом CUG назначается с помощью идентификатора, который включается в заголовок пакетов установления соединения коммутируемого виртуального канала. Без идентификатора CUG виртуальные соединения не будут устанавливаться с другими членами CUG. Это средство обеспечения безопасности имеет несколько режимов. В одном из них только члены CUG могут устанавливать виртуальные соединения друг с другом. Доступ за пределы группы CUG запрещен. Более того, доступ кого-либо извне также воспрещен. В другом режиме члены CUG могут устанавливать соединение с любым другим пользователем сети вне зависимости от того, является он или нет членом CUG. Однако установка соединений с членами группы CUG извне её запрещена. Хотя концепция группы CUG менее сложная и отличается от современных виртуальных частных сетей VPN (*Virtual Private Network*), между ними можно провести параллель. Для классической VPN характерно обеспечение не только защиты от несанкционированного доступа, но и выполнение требований по качеству обслуживания.

ГЛАВА 7. Структурные схемы программного обеспечения функций сетевого уровня сети X.25

Настоящая глава состоит из основной части, включающей структурные схемы программного обеспечения (ПО) процедур сетевого уровня сети X.25, и дополнения, включающего алгоритмы для составления ПО в двух лабораторных работах.

7.1. Структурная схема организации ПО функций сетевого уровня сети X.25

Все программы сетевого уровня *X.25* выполняются *центральным процессором* (Цпр) ЦКП и включают фоновые программы, диспетчер фоновых программ и программы обмена пакетами между Цпр и канальными процессорами. На рис. 7.1 приведена структурная схема организации ПО сетевого уровня X.25.

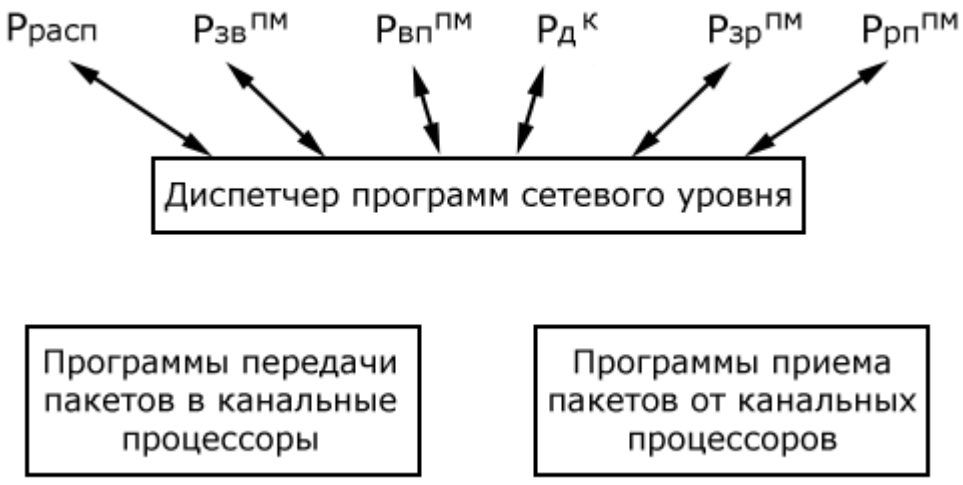


Рис. 7.1. Структурная схема организации ПО сетевого уровня в ЦКП

Основной принцип взаимодействия фоновых программ с диспетчером программ аналогичен тому, что было описано для канального уровня X.25 и заключается в последовательной обработке всех фоновых программ, большинство из которых выполняют функции обработки очередей массивов пакетов данных.

В настоящей главе приводится описание некоторых из фоновых программ, выполняемые вычислительными средствами ЦКП1 (рис. 7.2).

Структурные схемы этих программ составлены таким образом, что возврат к диспетчеру программ из фоновых программ происходит по завершению обработки всех пакетов в очереди. Такая организация ПО используется только для упрощения объяснения работы фоновых программ, хотя может быть не оптимальной.

Обозначим через j номер канального процессора, взаимодействующего с центральным процессором Цпр центра коммутации пакетов ЦКП. Тогда канальные процессоры ЦКП (см. рис. 7.2 и рис. 6.4 главы 6) Кпр1, Кпр2 и Кпр3 (взаимодействующие с оконечными станциями) имеют номера соответственно j=1, 2 и 3, а номера канальных процессоров Кпр4, Кпр5 и Кпр6 (взаимодействующие со смежным ЦКП) имеют номера соответственно j=4, 5 и 6. Обозначим очереди пакетов на приеме с канальных процессоров j через $О^{пм}(j)$. В нашем примере таких очередей шесть (по числу канальных процессоров). Обработанные центральным процессором $Ц_{ПР}$ пакеты устанавливаются в очереди $О^{пд}(j)$ пакетов на передачу в канальные процессоры. В нашем примере таких очередей также шесть (по числу канальных процессоров).

С помощью фоновой программы распределения $Р_{расп}$ из очередей $О^{пм}(j)$ формируются несколько очередей по типам пакетов («Запрос Вызова»; «Вызов Принят»; «пакеты данных, обрабатываемых по приоритету»; «пакеты данных, обрабатываемые без приоритета» и др.). Очереди пакетов «Запрос Вызова» (ЗВ) обозначим через $О_{зв}^{пм}(j)$. Она подлежит обработке фоновой программой $Р_{зв}^{пм}$. Очередь пакетов «Вызов Принят» (ВП) обозначим через $О_{в}^{пм}(j)$. Она подлежит обработке фоновой программой $Р_{вп}^{пм}$. Очереди пакетов данных (Д1), обрабатываемых по приоритету, обозначим через $О_{д1}^{пм}(j)$, а без приоритета (Д2) через $О_{д2}^{пм}(j)$. Обе очереди обрабатываются программой коммутации пакетов данные $Р_{д}^{к}$. Результатом работы всех приведенных фоновых программ приема (см. рис. 7.1) являются очереди $О^{пд}(j)$ пакетов на передачу в канальные процессоры.

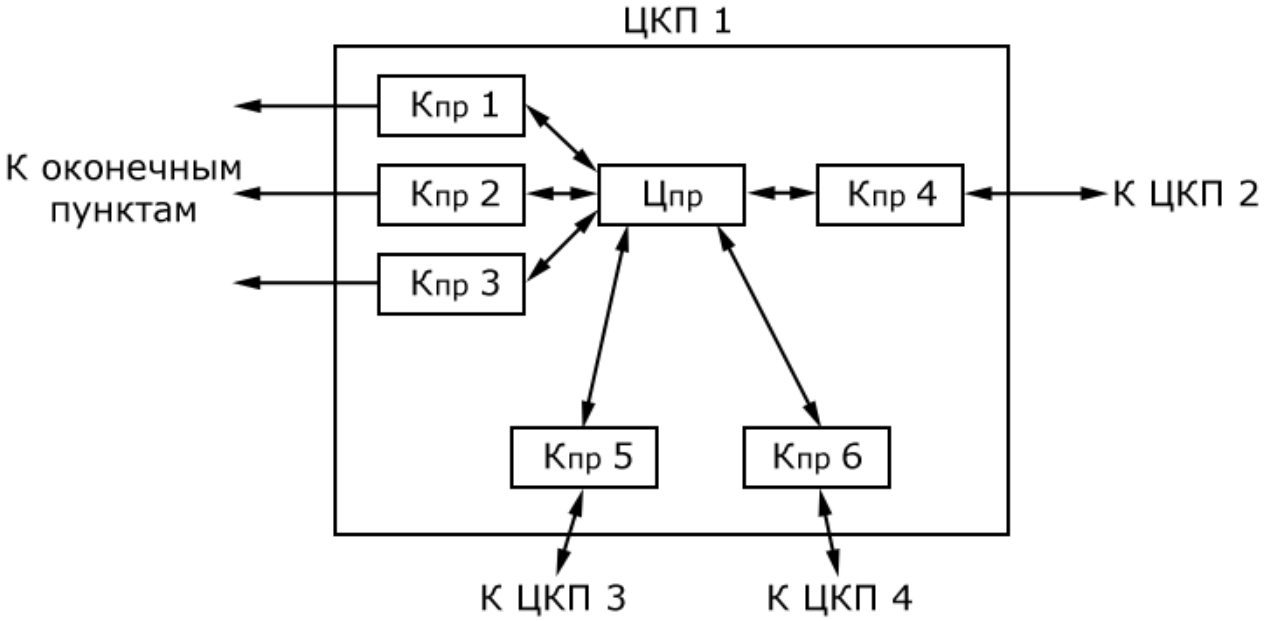


Рис. 7.2. Вычислительные средства ЦКП1

Приведем описание работы некоторых из фоновых программ (рис. 7.1) с помощью укрупненных структурных схем ПО. Для этого воспользуемся структурной схемой вычислительных средств ЦКП1, приведенной на рис. 7.2.

7.1.1. Структурная схема программы Ррасп «Распределение принятых пакетов из канальных процессоров в очереди по типам»

Из канальных процессоров пакеты поступают в центральный процессор Цпр. На рис. 7.3 приведена структурная схема программы Ррасп распределения этих пакетов в очереди по типам.

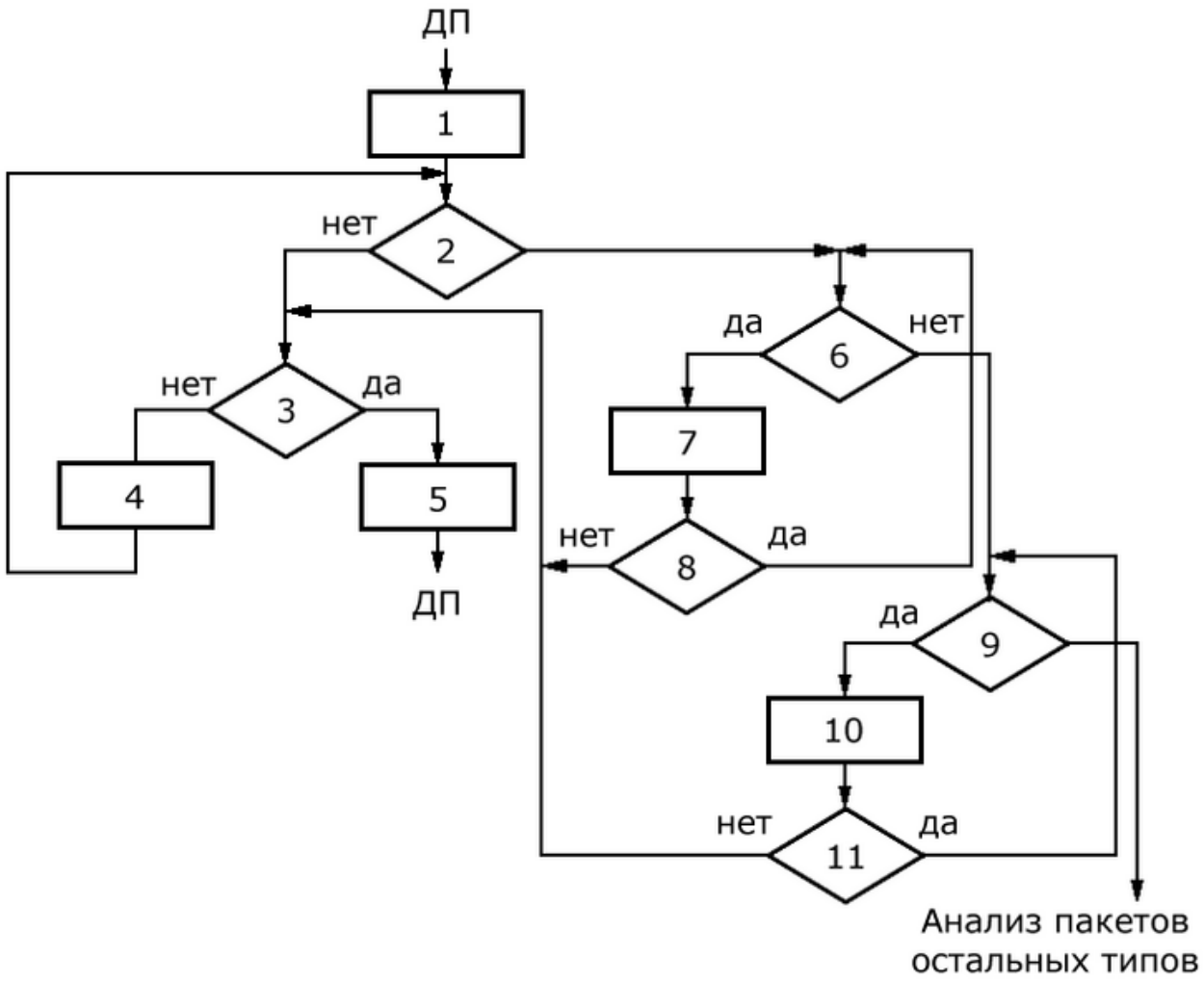


Рис. 7.3. Структурная схема программы $Р_{расп}$

Операция 1. Установить текущим канальный процессор с номером j=1.

Операция 2. Есть пакеты в очереди $О^{пм}$ (j) на приеме с канального процессора j? Если нет, то переход к операции 3. Иначе переход к операции 6.

Операция 3. Текущий канальный процессор является последним в ЦКП, т.е. j=Max? В примере рис. 7.2 Max=6. Если нет, то переход к операции 4, если да – к операции 5.

Операция 4. Переход к следующему канальному процессору j= j+1 и возврат к операции 2.

Операция 5. Установление текущим канальный процессор с номером j=1 и переход к диспетчеру программ.

Операция 6.Тип первого пакета в $О^{ПМ}$ (j) – «Запрос Вызова»? Если да, то переход к операции 7, иначе – к операции 9.

Операция 7. Снять первый пакет с $О^{ПМ}$ (j) и поставить в конец очереди $О_{зв}^{ПМ}$ (j) для обработки фоновой программой $Р_{зв}^{ПМ}$.

Операция 8. Есть пакеты в $О^{ПМ}$ (j)? Если нет, то переход к операции 3, иначе – переход к операции 6.

Операция 9-11. Аналогичны операциям 6-8, но при этом производится установка в очередь пакетов другого типа $О_{вп}^{ПМ}$ (j) («Вызов Принят») для обработки фоновой программой $Р_{вп}^{ПМ}$. Далее программа продолжает аналогично анализировать пакеты других типов.

7.2. Структурные схемы программ формирования таблицы маршрутизации по логическим канальным номерам LCN

Функцию формирования таблицы маршрутизации по логическим канальным номерам выполняют следующие программы:

- $Р_{зв}^{ПМ}$ «обработка принятых пакетов Запрос Вызова ЗВ» (рис. 7.4);
- $Р_{вп}^{ПМ}$ «обработка принятых пакетов Вызов Принят ВП» (рис. 7.5).

Последовательное выполнение этих программ формирует строку таблицы маршрутизации при установлении *коммутируемого виртуального канала* КВК (SVC).

7.2.1. Структурная схема программы “Обработка пакетов "Запрос Вызова"”

На рис. 7.4 приведена структурная схема программы "Обработка пакетов Запрос Вызова". Для рассмотрения принципа формирования строки таблицы маршрутизации по номерам логических каналов LCN допустим, что список очереди $О_{зв}^{ПМ}$ (j) состоит из следующих двух пакетов «ЗВ» (см. рис. 7.2).

Первый пакет в очереди поступил из ЦКП3 и через Кпр5 ЦКП1 коммутируется на Кпр4 для передачи в ЦКП2 (ЦКП3-Кпр5-Цпр ЦКП1-Кпр4-ЦКП2). Второй пакет в очереди поступил из

ЦКП2 и через Кпр4 ЦКП1 коммутируется на Кпр5 для передачи в ЦКП3 (ЦКП2-Кпр4-Цпр ЦКП1-Кпр5-ЦКП3).

Приведём описание формирования таблицы маршрутизации по LCN для соединения по первому пакету.

Операция 1. Есть пакет в $О^{пм}_{зв}$ (5), т.е. из Кпр5? Если нет, то переход к ДП. В нашем примере есть пакет в этой очереди. Поэтому переход к операции 2.

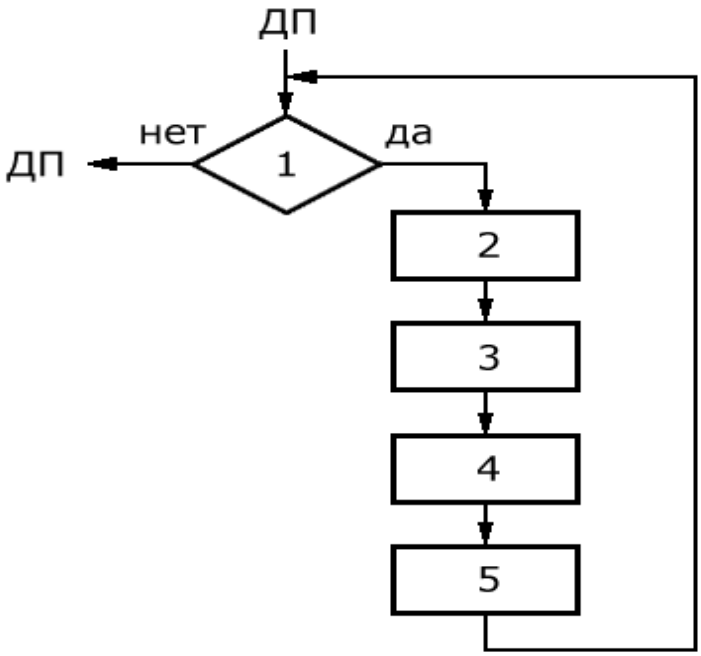


Рис. 7.4. Структурная схема программы “Обработка пакетов Запрос Вызова"

Операция 2. Обрабатывается первый пакет в $О^{пм}_{зв}$ (5). С помощью таблицы маршрутизации физических адресов (нумерация стандартизирована протоколом X.121) определяется номер канального процессора, на который должен быть скоммутирован входящий пакет с установленным в нем LCN=179. В нашем примере таким канальным процессором Кпр=4 ЦКП1. На этот процессор пакет должен поступить с измененным уникальным номером LCN (см. главу 6).

Операция 3. Для определения LCN с целью замены им в исходящем пакете используется очередь свободных номеров Освн, создаваемая в каждом ЦКП. На рис. 7.5

приведена Освн в исходном состоянии перед началом работы. В этом случае она содержит последовательные номера от 1 до 4094, т.е. по максимальному числу виртуальных каналов через ЦКП в сети X.25 (два резервного номера).

В процессе работы сети при установлении КВК свободные номера берутся из этой очереди Освн, а при разрыве КВК устанавливаются в хвост этой очереди, т.е. номера не будут такими упорядоченными (т.е. последовательными), как приведено на рис. 7.5. Определяем для исходящего первого пакета «ЗВ» LCN. Допустим, в этот момент первым в Освн был LCN=3201. Считываем этот LCN из Освн. Использование списка очередей позволяет сократить число команд на поиск свободного номера.

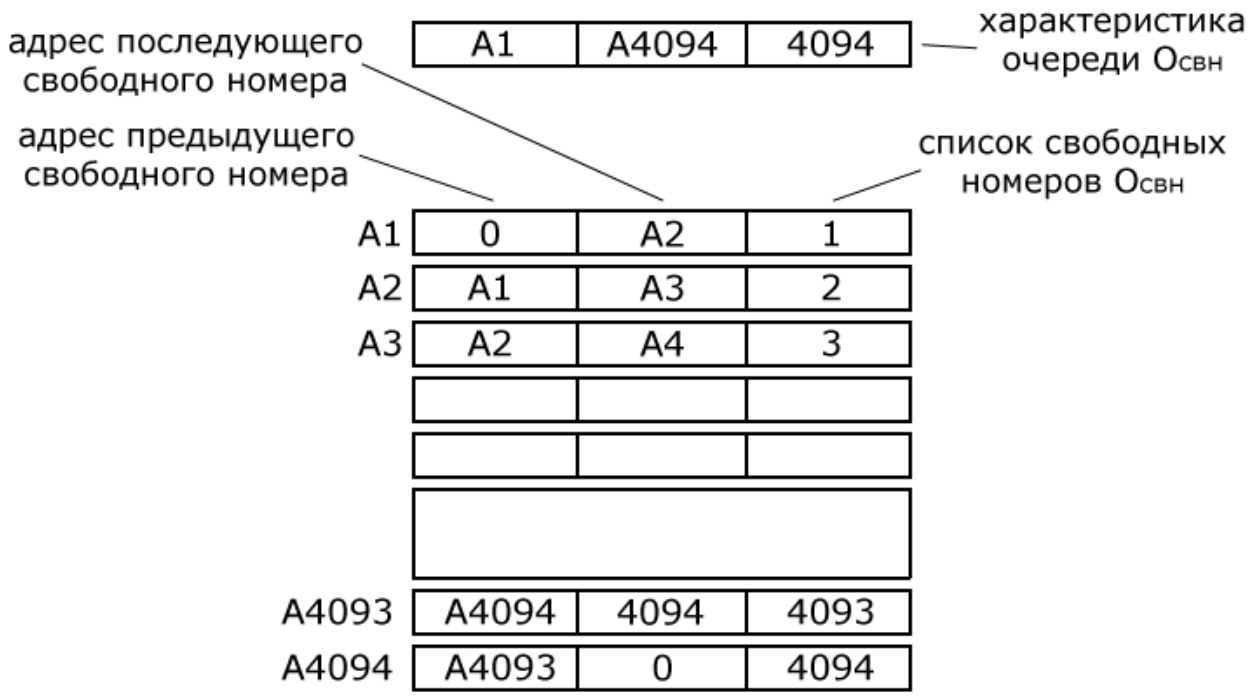


Рис. 7.5. Очередь свободных номеров перед началом работы ЦКП

Операция 4. Заполняем строку таблицы 7.1 маршрутизации по LCN для пакета, входящего из Кпр5, учитывая приведенные выше значения: LCN входящего пакета (179); LCN исходящего пакета (3201); номер Кпр исходящего пакета (Кпр4).

Табл. 7.1. Таблица маршрутизации ЦКП1 по LCN для пакетов из Кпр5

LCN входящего	LCN исходящего	Номер канального процессора исходящего	Признак использования Освн при формировании строки

пакета в ЦКП1	пакета в ЦКП1	пакета из ЦКП1	таблицы маршрутизации (да/нет)
179	3201	Кпр4	Да
193	220	Кпр4	нет

В таблице 7.1 введен еще один столбец, указывающий на то, что при формировании строки таблицы маршрутизации использовалась ли Освн для получения LCN исходящего пакета из ЦКП. Фоновая программа $Р^{пм}_{зв}$ выполняет эту операцию. Как будет показано ниже программа $Р^{пм}_{вп}$ «Обработка принятых пакетов Вызов Принят - ВП» эту операцию не выполняет. Из приведенных в табл. 7.1 двух строк маршрутизации только первая строка формируется программой $Р^{пм}_{зв}$. При разъединении виртуального канала следует установленный этой программой LCN вернуть в Освн. Вторая строка таблицы 7.2 формируется программой $Р^{пм}_{вп}$ при установлении виртуального соединения с помощью пакета "ВП" из ЦКП 2 в ЦКП 3. Как показано в главе 6, пакет "ВП" коммутируется по строке маршрутизации логических номеров, сформированной пакетом «ЗВ» этого виртуального канала и является подтверждением установления виртуального канала. При формировании этой строки таблицы маршрутизации не использовалась Освн для получения LCN исходящего пакета из ЦКП.

Операция 5. Снять первый из $О^{пм}_{зв}$ (5) и поставить в хвост очереди на передачу пакетов в канальный процессор Кпр4, т.е. $О^{пд}$(4).

Табл.7.2. Таблица маршрутизации ЦКП1 по LCN для пакетов из Кпр4

LCN входящего пакета в ЦКП	LCN исходящего пакета в ЦКП	Номер канального процессора исходящего пакета из ЦКП	Признак использования Освн при формировании строки таблицы маршрутизации (да/нет)
220	193	Кпр5	Да
3201	179	Кпр5	нет

7.2.2. Структурная схема программы “Обработка пакетов "Вызов Принят""”

Рассмотрим работу программы $Р_{вп}^{пм}$ – обработка принятых пакетов «Вызов Принят - ВП» по структурной схеме рис. 7.6.

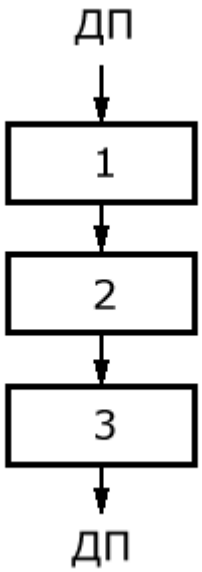


Рис. 7.6. Структурная схема программы $Р_{вп}^{пм}$ – обработка принятых пакетов «Вызов Принят - ВП»

Программа $Р_{вп}^{пм}$ формирует еще одну строку таблицы маршрутизации ЦКП по LCN. Пакет «ВП» направляется в противоположную сторону той, в которую передавался пакет «ЗВ» при установлении виртуального канала. При этом коммутация пакетов «ВП» производится на основании тех LCN, которые были выбраны из Освн программой $Р_{вп}^{пм}$. Покажем работу программы $Р_{вп}^{пм}$ на примере обработки одного пакета «ВП», поступившего при установлении виртуального канала в ответ на пакет «ЗВ». В качестве такого пакета примем пакет «ВП», являющийся результатом обработки первого пакета в $О_{зв}^{пм}$ и сформировавшего строку таблицы маршрутизации с LCN входящего и исходящего пакета ЦКП соответственно 179 и 3201 (табл. 7.1).

Операция 1. Обрабатывается первый пакет в $О_{вп}^{пм}$ (4). Этот пакет «ВП» поступает с Кпр4 с LCN=3201(табл. 7.2). Определяем строку таблицы маршрутизации с этим LCN.

Операция 2. По этой строке определяем, что LCN исходящего из ЦКП этого пакета

изменяется на LCN=179 (табл. 7.2).

Обращаем внимание, что сформированная строка маршрутизации в табл. 7.2 использует ту же LCN, которая была определена программой $Р^{пм}_{вп}$ из Освн. По этой строке определяем, что этот пакет из Кпр4 коммутируется на Кпр5. При этом Освн не используется.

Операция 3. Снять первый из $О^{пм}_{вп}$ (4) и поставить в хвост очереди на передачу пакетов в канальный процессор Кпр5, т.е. $О^{пд}$(5).

В таблицах 7.1 и 7.2 приведены результаты формирования таблицы маршрутизации по LCN для второго пакета "ЗВ" из ЦКП 2 в ЦКП 3. Как видно из таблиц для этого виртуального соединения LCN=193 и 220.

Теперь на основании таблиц 7.1 и 7.2 составляется единая таблица маршрутизации ЦКП по LCN (табл. 7.3).

Таблица 7.3. Таблица маршрутизации ЦКП

Номер канального процессора пакета, входящего в ЦКП	Номер канального процессора пакета, исходящего из ЦКП	LCN входящего пакета в ЦКП	LCN исходящего пакета из ЦКП	Признак использования Освн при формировании строки таблицы маршрутизации (да/нет)
4	5	220	193	да
4	5	3201	179	нет
5	4	179	3201	да
5	4	193	220	нет

7.3. Структурная схема программы "Коммутация пакетов "данные""

На рис. 7.7 приведена упрощенная структурная схема программы "Коммутация пакетов "данные" $Рд^{к}$ ". Рассматривается прием пакетов только с одного канального процессора.

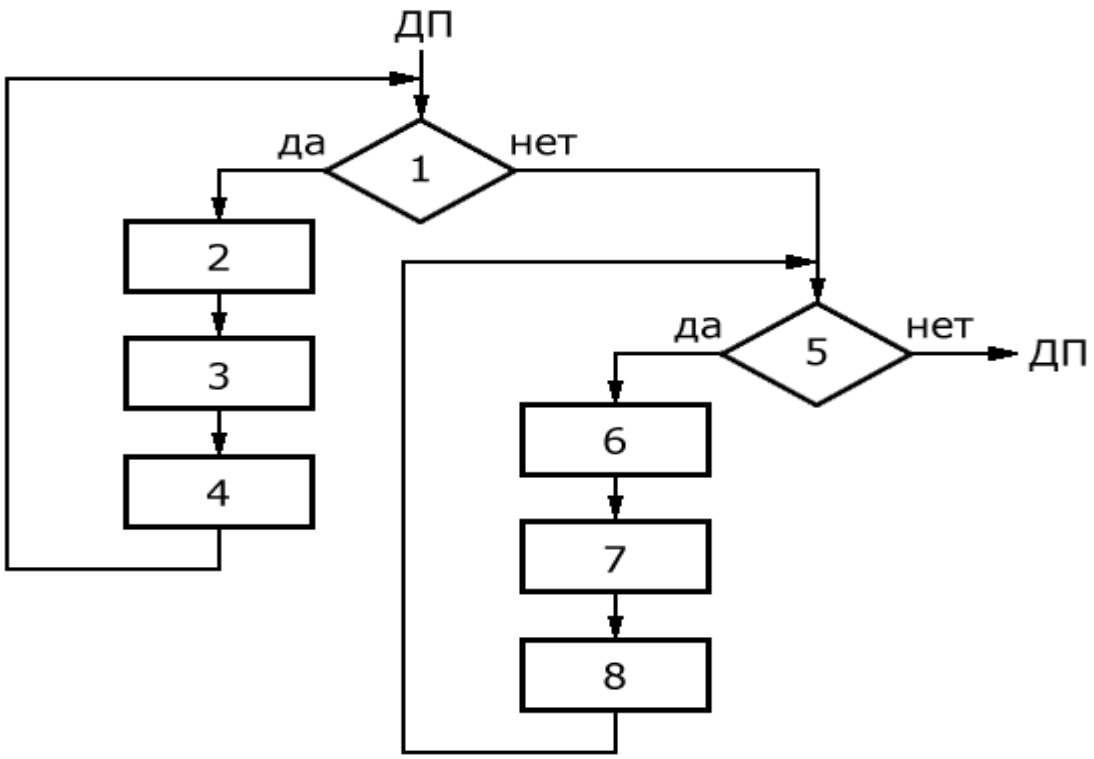


Рис. 7.7. Структурная схема программы "Коммутация пакетов "данные" $Р_{Д}^{К}$ "

Операция 1. Есть ли пакеты в $О_{д1}^{пм}(j)$, обрабатываемые по приоритету? Если да, то переход к операции 2, иначе переход к операции 5.

Операция 2. Определяется LCN первого пакета в очереди $О_{д1}^{пм}(j)$, который подлежит коммутации в Цпр ЦКП.

Операция 3. По таблице маршрутизации ЦКП (табл. 7.3) на основании номера канального процессора, с которого пакет поступает в Цпр ЦКП, и значения LCN в его заголовке определяется:

- номер канального процессора, на который должен быть скоммутирован этот первый пакет;
- LCN в заголовке этого пакета после его коммутации в ЦКП.

Операция 4. Снять первый пакет из $О_{д1}^{пм}(j)$ и поставить его в хвост очереди пакетов на

передачу в канальный процессор j, определённый в операции 3, т.е. $О^{пд}(j)$. Установить в этот пакет LCN, определённый в операции 3. Возврат к операции 1.

Операция 5. Есть ли пакеты в $О_{д2}^{пм}(j)$, обрабатываемые без приоритета? Если да, то переход к операции 6, иначе - в ДП.

Операции 6 - 8 аналогичны операциям 2 - 4, за исключением:

- анализируются пакеты "данные" $О_{д2}^{пм}(j)$, а не $О_{д1}^{пм}(j)$;
- по завершении операции 8 возврат к операции 5.

Дополнение. Алгоритмы реализации программ для использования в лабораторных работах

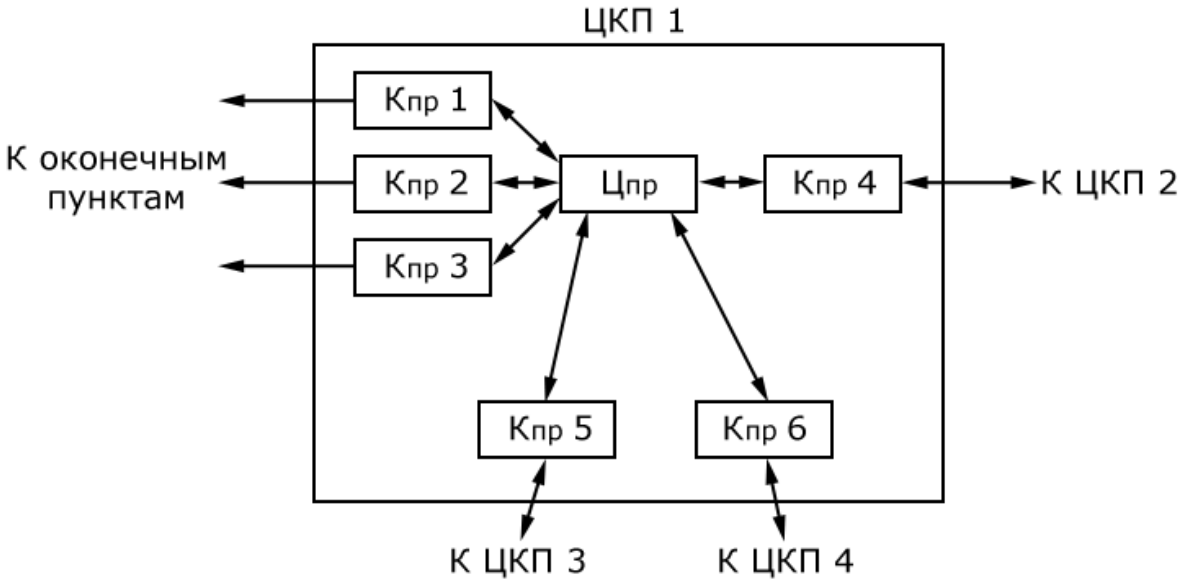
Настоящее дополнение включает предлагаемые алгоритмы реализации двух программ для использования их в лабораторных работах.

Лабораторная работа №7

Алгоритм программы формирования таблицы маршрутизации на сетевом уровне

Программа LAB7

Программа LAB7 выполняет функции структурных схем программ формирования таблицы маршрутизации по логическим канальным номерам LCN (см. глава 7). Эти схемы в указанной главе составлены на примере структуры центра коммутации пакетов, приведенном на этом рисунке.



Описание:

- константы N1, N3;
- переменные D, $К_{ПР,}$ i, j, Y, LCN;
- массивы LCN (i), LCN1 (i);
- программы DISP7, P_1, P_2, P_3, P_4, P_5, P_6, P_7**;**
- очереди $О_{своб.}$, $О_{свн}$, $О_{ЗВ}^{пм}$ (5), $О^{пд}$ (4), $О_{ВП}^{пм}$ (4), $О^{пд}$ (5).

Диспетчер программы DISP7

Begin

D:= 1

IF D = 1 THEN GO TO P_1 ELSE IF D = 2 THEN GO TO P_2 ELSE

IF D= 3 THEN GO TO P_3 ELSE IF D = 4 THEN GO TO P_4 ELSE

IF D = 5 THEN GO TO P_5 ELSE IF D = 6 THEN GO TO P_6 ELSE IF D =7 THEN GO TO P_7

ELSE

END

Программы:

P_1 – формирование очереди из N1 свободных блоков;

P_2 – формирование N3 пакетов “Запрос Вызова” (ЗВ), находящихся в очереди принятых пакетов с канального процессора $К_{ПР}$=5;

P_3 – формирование очереди свободных номеров $О_{свн}$ из очереди свободных блоков $О_{своб.}$ и запись в них значений для использования в качестве логического канального номера LCN;

P_4 – перенос пакет ЗВ из очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=5) $О_{ЗВ}^{пм}$ (5) в очередь пакетов на передачу в канальный процессор 4 – $О^{пд}$ (4);

P_5 – формирование строки таблицы маршрутизации в Центре Коммутации Пакетов (ЦКП);

P_6 – формирование одного пакета “Вызов Принят” (ВП), находящегося в очереди принятых пакетов с канального процессора $К_{ПР}$=4;

P_7 – перенос пакета ВП из очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=4) $О_{ВП}^{пм}$ (4) в очередь пакетов на передачу в канальный процессор 5 – $О^{пд}$ (5).

По окончании работы программы по исходным данным контрольного примера P_7 необходимо

показать результат:

- содержание полей пакетов (LCN в побитовой и десятичной форме, идентификатор пакета и адреса в побитовой форме) в очередях $О^{пд}(4)$, $О^{пд}(5)$;
- содержание массивов блоков очереди свободных номеров $О_{свн}$;
- содержание сформированной таблицы маршрутизации (табл. 2).

7.1. Программа $Р_1$

а) Выделение памяти под N1 свободных блоков (для всех вариантов и контрольного примера N1=50). Каждый свободный блок занимает 34 байта:

- 2 байта под адрес предыдущего блока в списке блоков (первое адресное поле связки очереди);
- 2 байта под адрес следующего блока в списке блоков (второе адресное поле связки очереди);
- 30 байт под пакеты установления и сброса соединения (Запрос Вызова, Вызов Принят и др.);

Очистить память, занятую свободными блоками.

б) Установление адресов связки в N1 свободных блоках:

- выделить память под характеристику очереди свободных блоков $Н_{своб}$ с начальным адресом $АН_{своб.}$ Установить поля характеристики $Н_{своб}$ (рис.1).

$АН_{своб}$

A(1)	A(N1)	N1

Рис.1. Характеристика $Н_{своб}$

Здесь:

A(1) – адрес начала массива первого свободного блока в очереди $О_{своб}$;

A(N1) – адрес начала массива последнего свободного блока в очереди $О_{своб.}$

Под массивом блока будем понимать блок (пакет, кадр, ячейка и др.) с адресными полями связки очереди.

Установить адресные поля связки первого (рис. 2, а) и N1 – го (рис. 2, б) свободного блока в очереди $О_{своб.}$

A(1)

0	A(N1)	

а)

A(N1)

A(N1) -1	0	

б)

Рис. 2. Формат массивов первого (а) и последнего (б) свободного блока в очереди $О_{своб}$

Установить адреса связки массивов всех свободных блоков, кроме первого и последнего.

FOR i=2, 3 …. (N1-1) DO

Запись в первое адресное поле массива i-го блока адрес начала массива i-1 блока списка очереди;

Запись во второе адресное поле массива i-го блока адрес начала массива i+1 блока списка очереди.

i=i+1

END

D:=D+1

GO TO DISP7

7.2. Программа $Р_2$

Запишем в центральный процессор N3 пакетов “Запрос Вызова” ”, поступивших с канального процессора j=5 (т.е. $К_{ПР}$=5), в первые массивы очереди свободных блоков $О_{своб}$. В контрольном примере N3=3.

На рис. 3 показано формат полей массива пакета с начальным адресом A(i) “Запрос Вызова” (ЗВ), размещенного в $О_{своб}$.

Число байт	2	2	30
Начальный адрес A(i)	Первое адресное	Второе адресное	“Запрос Вызова” – логический канальный номер LCN 12 бит (биты <1- 8> 1 байта и биты <5-8> 2 байта),

	поле	поле	идентификатор пакета – 4 бита 1011 (биты <1- 4> 2 байта), адрес вызываемого – 14 (1+3+10) байт, адрес вызывающего – 14 (1+3+10) байт

Рис. 3. Формат полей пакета “Запрос Вызова” в массиве свободного блока очереди $О_{своб}$

Примечание: биты <5-8> 2 байта LCN являются младшими.

Установим значение полей этих пакетов “Запрос Вызова” .

Значения LCN этих пакетов запишем в виде следующего одномерного массива - LCN (i) = 179, 195, 201. Здесь i- номер пакета ЗВ.

FOR i= 1,2…..N3 DO

Записать в поле пакета “ЗВ” с начальным адресом массива A(i): биты <1-8> 1 байта и биты <5-8> 2 байта:= LCN(i), биты <1- 4> 2 байта:= 1011; в каждые 14 байт с начиная с третьего записать значение i (адрес вызывающего абонента), в каждые 14 байт с начиная с 17-го записать значение i+1 (адрес вызываемого абонента),

END

В результате в N3 пакетах “ Запрос Вызова ”, находящиеся в $О_{своб}$ с начальными адресами массивов A(1), A(2), A(3), записаны соответственно следующие логические канальные номера LCN=179, 195 и 201.

Перенести массивы этих N3 пакетов из $О_{своб}$ в очередь массивов принятых пакетов $О_{ЗВ}^{ПМ}$ (5) с канального процессора j=5, т.е. $К_{ПР}$=5.

Откорректировать очередь свободных блоков $О_{своб}$, создать $О_{ЗВ}^{ПМ}$ (5) и характеристики $Н_{своб}$, $Н_{ЗВ}^{ПМ}$ (5). На рис. 4 приведена характеристика этой очереди $Н_{своб.}$ Корректировка и создание очередей здесь не показана.

$АН_{своб.}$

A(N3+ 1)	A(N 1)	N1- N3

Рис.4. Характеристика $Н_{своб.}$

На рис. 5 приведена характеристика очереди $Н_{ЗВ}^{ПМ}$ (5).

$АН_{ЗВ}^{ПМ}$ (5)

A(1)	A(N 3)	N3

Рис.5. Характеристика $Н_{ЗВ}^{ПМ}$ (5)

D:=D+1
GO TO DISP7

7.3. Программа $Р_3$

Создать очередь свободных номеров $О_{свн}$ из очереди свободных блоков $О_{своб.}$ Принять число свободных номеров для всех вариантов и контрольного примера Y=20. . Корректировка и создание очередей здесь не показана.

Установить характеристику $Н_{свн}$ очереди свободных номеров $О_{свн}$ (рис.6)

$АН_{свн}$

A(N3+ 1)	A(N3+2 0)	2 0

Рис.6. Характеристика $Н_{свн}$

Откорректировать очередь массивов свободных блоков $О_{своб.}$ На рис. 7 приведена характеристика этой очереди $Н_{своб}$

$АН_{своб}$

A(N3+20+1)	A(N1)	N1- N3 - 20

Рис.7. Характеристика $Н_{своб}$

На рис. 8 приведен формат массива блока свободных номеров.

Байты	2	2	2
Значение	Начальный адрес предыдущего блока	Начальный адрес следующего блока	Значение свободного номера для записи LCN

Рис. 8. Формат массива свободного номера

Установить значения одномерного массива свободных номеров для шести (для упрощения из 20) значений LCN1 (i) = 3201, 220, 4072, 3701, 475, 432.

Записать в шесть массивов блоков очереди свободных номеров $О_{свн}$ эти значения свободных логических канальных номеров LCN

FOR i= 1, 2…..6 DO
Записать в поле значения свободного номера массива свободных номеров (рис. 8) с начальным адресом A(N3+i):= LCN1(i)
END

Заменить значения логических канальных номеров LCN во всех N3 принятых пакетах $О_{ЗВ}^{ПМ}$ (5) с канального процессора $К_{ПР}$=5 на значения, взятые из очереди свободных номеров $О_{свн.}$

FOR i= 1,2…..N3 DO
Записать в поле пакета “ЗВ” с начальным адресом массива A(i): биты <1-8> 1 байта и биты <5-8> 2 байта:= A(N3+i)
END

- откорректировать очередь $О_{свн}$ и характеристику $Н_{свн}$.

Корректировка очереди здесь не показана. Массивы свободных номеров, начиная с A(N3+1) по A(N3+ N3) пересылаются в отдельную очередь занятых номеров, которая для упрощения здесь не показана. На рис. 9 показана характеристика $Н_{свн.}$

$АН_{свн}$

A(N3+ N3+1)	A(N3+20)	20- N3

Рис.9. Характеристика $Н_{свн}$

D:=D+1

GO TO DISP7

7.4. Программа P_4

В настоящей работе ограничимся установлением одной строки таблицы маршрутизации по логическим канальным номерам (Примечание. В очереди $О_{ЗВ}^{ПМ}$ (5) стоят N3 пакета ЗВ)

С помощью таблицы маршрутизации физических номеров на основании значений адресов (рис. 3) вызываемого и вызывающего пользователя (каждый длиной 14 байт) находим номер канального процессора, на который должен быть скоммутирован первый принятый пакет ЗВ. Этот пакет стоит первым в очереди массивов принятых пакетов $О_{ЗВ}^{ПМ}$ (5) с канального процессора $К_{ПР}$=5 с логическим канальный номером LCN – 3201 (программа P_3). В примере (глава 7) номер канального процессора 4, на который должен быть скоммутирован этот пакет ЗВ. Программно здесь это не реализовано. В очередь пакетов на передачу в канальный процессор 4 – $О^{ПД}$ (4) должен быть перенесен этот пакет ЗВ из очереди массивов принятых пакетов $О_{ЗВ}^{ПМ}$ (5).

На рис. 10 приведено содержание полей массива этого пакета ЗВ (не указаны адреса вызывающего и вызываемого абонента).

Число байт	2	2	30
Начальный адрес А(1)	Первое адресное поле - 0	Второе адресное поле - 0	101000000001 (логический канальный номер LCN-3201), 1011 (идентификатор пакета ЗВ), адрес вызываемого – 14 байт, адрес вызывающего – 14 байт

Рис. 10. Массив пакета “Запрос Вызова” в очереди пакетов на передачу в канальный процессор 4 – $О^{ПД}$ (4)

Установить характеристику очереди (рис.11) пакетов на передачу в канальный процессор 4 – $Н^{ПД}$ (4). Поскольку в настоящем примере в этой очереди один пакет, то значения адресных полей массива пакета ЗВ в этой очереди равны нулю.

$АН^{ПД}$ (4)

А(1)	А(1)	1

Рис.11. Характеристика $Н^{ПД}$ (4)

Откорректировать очередь массивов принятых пакетов $О_{ЗВ}^{ПМ}$ (5) с канального процессора $К_{ПР}$=5. Корректировка очереди здесь не показана.

На рис. 12 показана характеристика $Н_{ЗВ}^{ПМ}$ (5) .

$АН_{ЗВ}^{ПМ}$ (5).

A(2)	A(N 3)	N3-1

Рис.12. Характеристика $Н_{ЗВ}^{ПМ}$ (5)

D:=D+1

GO TO DISP

7.5. Программа P_5

В таблице 1 приведена строка маршрутизации по логическим канальным номерам LCN, полученная в результате работы программ P_1- P_4 по обработке пакета “Запрос Вызова” и в соответствии с алгоритмом, изложенным в главе 7.

В столбце 5 отмечается, что при формировании этой строки LCN в пакете на выходе ЦКП было установлено с использованием свободного номера из очереди Освн.

Таблица 1. Таблица маршрутизации ЦКП

1	2	3	4	5
Номер канального процессора пакета, входящего в ЦКП	Номер канального процессора пакета, исходящего из ЦКП	LCN входящего пакета в ЦКП	LCN исходящего пакета из ЦКП	Признак использования Освн при формировании строки таблицы маршрутизации (да/нет)
5	4	179	3201	да

D:=D+1
GO TO DISP7

7.6. Программа P_6

На рис. 13 показан формат полей принятого одного пакета “Вызов Принят” (ВП) из канального процессора $К_{ПР}$=4, размещенного в первом свободном блоке $О_{своб}$. Этот пакет является квитанцией на пакет ЗВ, который сформировал строку таблицы маршрутизации виртуального канала связи (табл.1).

Число байт	2	2	30
Начальный	Первое	Второе	“Вызов Принят” – логический канальный номер LCN

адрес A(i)	адресное поле	адресное поле	12 бит (биты <1-8> 1 байта и биты <5-8> 2 байта), идентификатор пакета – 4 бита 1111 (биты <1-4> 2 байта), адрес вызываемого – 14 (1+3+10) байт, адрес вызывающего – 14 (1+3+10) байт

Рис. 13. Формат размещения пакета “Вызов Принят” в свободном блоке $О_{своб}$ с начальным адресом A(i)

Установим значение полей пакета “Вызов Принят” в первом массиве блоков очереди $О_{своб.}$ Согласно рис. 7 начальный адрес такого массива A(N3+21). В первых 12 битах этого пакета в десятичном отображении LCN = 3201 в соответствии с табл.7.1. Поля адресов вызывающего и вызываемого те же, что и в ранее обработанном пакете ЗВ.

Откорректировать очередь $О_{своб.}$ Корректировка очереди здесь не показана.

. На рис. 14 приведена характеристика этой очереди $Н_{своб.}$

$АН_{своб.}$

A(N3+22)	A(N1)	N1- N3 - 21

Рис.14. Характеристика $Н_{своб}$

В результате в первых N3 свободных блоках установлены пакеты “Вызов Принят” (ВП). Перенести массив пакета ВП из очереди $О_{своб.}$ в очередь массивов принятых пакетов $О_{ВП}^{ПМ}$ (4) с канального процессора $К_{ПР}$=4. Откорректировать $О_{ВП}^{ПМ}$ (4). . Корректировка очереди здесь не показана.

Установить характеристику очереди $Н_{ВП}^{ПМ}$ (4) массивов принятых пакетов $О_{ВП}^{ПМ}$ (4) с канального процессора $К_{ПР}$=4.

На рис. 15 приведена характеристика очереди $Н_{ВП}^{ПМ}$ (4).

$АН_{ВП}^{ПМ}$ (4)

A(N3+21)	A(N3+21)	1

Рис.15. Характеристика $Н_{ВП}^{ПМ}$ (4)

D:=D+1
GO TO DISP7

7.7. Программа P_7

Перенести первый пакет ВП из очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=4) $О_{ВП}^{ПМ}$ (4), который находится по адресу A(N3+21) первого поля характеристики этой очереди (рис. 15) в очередь пакетов на передачу в канальный процессор 5 – $О^{пд}$ (5). Прежде, чем перенести этот пакет ЗВ на основании таблицы маршрутизации ЦКП (табл. 1) в нем необходимо заменить LCN=3201 на значение LCN=179 (10110011), т.е. записать в первые 12 бит пакета ВП (рис. 13). Установить характеристику очереди (рис.16) пакетов на передачу в канальный процессор 5 – $Н^{пд}$ (5). Поскольку в настоящем примере в этой очереди один пакет, то значения адресных полей массива пакета ВП в этой очереди равны нулю.

$АН^{пд}$ (4)

A(N3+21)	A(N3+21)	1

Рис.16. Характеристика $Н^{пд}$ (5)

В результате обработки пакета ВП в таблицу маршрутизации ЦКП добавляется еще одна строка маршрутизации. В столбце 5 отмечается, что при формировании этой строки LCN в пакете на выходе ЦКП было установлено без использования свободного номера из очереди Освн.

Таблица 2. Таблица маршрутизации ЦКП

1	**2**	**3**	**4**	**5**
Номер канального процессора пакета, входящего в ЦКП	Номер канального процессора пакета, исходящего из ЦКП	LCN входящего пакета в ЦКП	LCN исходящего пакета из ЦКП	Признак использования Освн при формировании строки таблицы маршрутизации (да/нет)

5	4	179	3201	да
4	5	3201	179	нет

- откорректировать характеристику очереди $Н_{ВП}^{ПМ}(4)$ массивов принятых пакетов $О_{ВП}^{ПМ}(4)$ с канального процессора $К_{ПР}=4$ в результате снятия первого пакета ВП из очереди массивов принятых пакетов (с канального процессора $К_{ПР}=4$) $О_{ВП}^{ПМ}(4)$.

D:=D+1
GO TO DISP7

7.8. Исходные данные для лабораторной работы

В таблице 3 приведены исходные данные пяти вариантов лабораторной работы и контрольного примера

Таблица 3. Исходные данные для лабораторной работы

Параметр	1 вариант	2 вариант	3 вариант	4 вариант	5 вариант	Контрольный вариант
N1	40	40	40	40	40	50
N3	3	3	2	4	2	3
m	2	3	4	5	6	1

Некоторые характеристики контрольного примера

$АН_{своб.}$

A(4)	A(50)	47

Рис.4. Характеристика $Н_{своб.}$

$АН_{ЗВ}^{ПМ}(5)$

A(1)	A(3)	3

Рис.5. Характеристика $Н_{ЗВ}^{ПМ}(5)$

$АН_{свн}$

A(4)	A(23)	20

Рис.6. Характеристика $Н_{свн}$

$АН_{своб.}$

A(24)	A(50)	27

Рис.7. Характеристика $Н_{своб.}$

$АН_{свн}$

A(7)	A(23)	17

Рис.9. Характеристика $Н_{свн}$

$АН_{ЗВ}^{ПМ}$ (5).

A(2)	A(3)	2

Рис.12. Характеристика $Н_{ЗВ}^{ПМ}$ (5)

$АН_{своб.}$

A(25)	A(50)	26

Рис.14. Характеристика $Н_{своб}$

$АН_{ВП}^{ПМ}$ (4)

A(N3+21)	A(24)	1

Рис.15. Характеристика $Н_{ВП}^{ПМ}$ (4)

$АН^{ПД}$ (4)

A(24)	A(24)	1

Рис.16. Характеристика $Н^{ПД}$ (5)

Лабораторная работа №8

Алгоритм программы "Коммутация пакетов "данные"

Программа LAB8
Программа LAB8 выполняет функции структурной схемы программы Коммутация пакетов "данные" (см. глава 7).

Описание:
- константы N1, *m, n*;
- переменные D, i, $К_{ПР}$, LCN;
- программы DISP7, P_1, P_2, P_3, P_4, P_5**;**
- очереди $О_{своб}$, $О_Д^{пм}$ (5), $О^{пд}$ (4), $О_Д^{пм}$ (4), $О^{пд}$ (5).

Диспетчер программы DISP8
Begin
D:= 1
IF D = 1 THEN GO TO P_1 ELSE IF D = 2 THEN GO TO P_2 ELSE
IF D= 3 THEN GO TO P_3 ELSE IF D= 4 THEN GO TO P_4 ELSE
IF D= 5 THEN GO TO P_5 ELSE
END
Программы:
P_1 – формирование очереди из N1 свободных блоков.
P_2 – формирование двух пакетов “Данные” (Д), находящихся в очереди принятых пакетов с канального процессора $К_{ПР}$=5.
P_3 – перенос пакетов Д из очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=5) $О_Д^{пм}$ (5) в очередь пакетов на передачу в канальный процессор.
P_4 – формирование двух пакетов “Данные” (Д), находящихся в очереди принятых пакетов с канального процессора $К_{ПР}$=4.
P_5 – перенос пакетов Д из очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=4) $О_Д^{пм}$ (4) в очередь пакетов на передачу в канальный процессор.

По окончании работы программы по исходным данным контрольного примера P_5 необходимо показать результат:

содержание в побитовой и десятичной форме полей пакетов (LCN, информационной части) в очередях $О^{пд}$ (4), $О^{пд}$ (5).

8.1. Программа P_1

а) Выделение памяти под N1 свободных блоков (для контрольного примера N1=50). Каждый свободный блок занимает 134 байта:
- 2 байта под адрес предыдущего блока в списке блоков (первое адресное поле связки очереди);
- 2 байта под адрес следующего блока в списке блоков (второе адресное поле связки очереди);

- 12 бит под логический канальный номер LCN
- 4 бит под тип пакета «данные»;
- 128 байт информационных данных пакета.

Очистить память, занятую свободными блоками.

б) Установление адресов связки в N1 свободных блоках:

- выделить память под характеристику очереди свободных блоков $Н_{своб}$ с начальным адресом $АН_{своб.}$ Установить поля характеристики $Н_{своб}$ (рис.1).

$АН_{своб}$

A(1)	A(N1)	N1

Рис.1. Характеристика $Н_{своб}$

Здесь

A(1) – адрес начала массива первого свободного блока в очереди $О_{своб}$

A(N1) – адрес начала массива последнего свободного блока в очереди $О_{своб.}$

Под массивом блока будем понимать блок (пакет, кадр, ячейка и др.) с адресными полями связки очереди.

- установить адресные поля связки первого (рис. 2, а) и N1 – го (рис. 2, б) свободного блока в очереди $О_{своб.}$

A(1)

0	A(N1)	

а)

A(N1)

A(N1) -1	0	

б)

Рис. 2. Формат первого (а) и последнего (б) свободного блока в списке очереди $О_{своб.}$

- установить адреса связки всех свободных блоков, кроме первого и последнего

FOR i=2, 3 …. (N1-1) DO
Запись в первое адресное поле i-го блока адрес начала i-1 блока списка очереди;
Запись во второе адресное поле i-го блока адрес начала i+1 блока списка очереди.
i=i+1
END

D:=D+1
GO TO DISP8

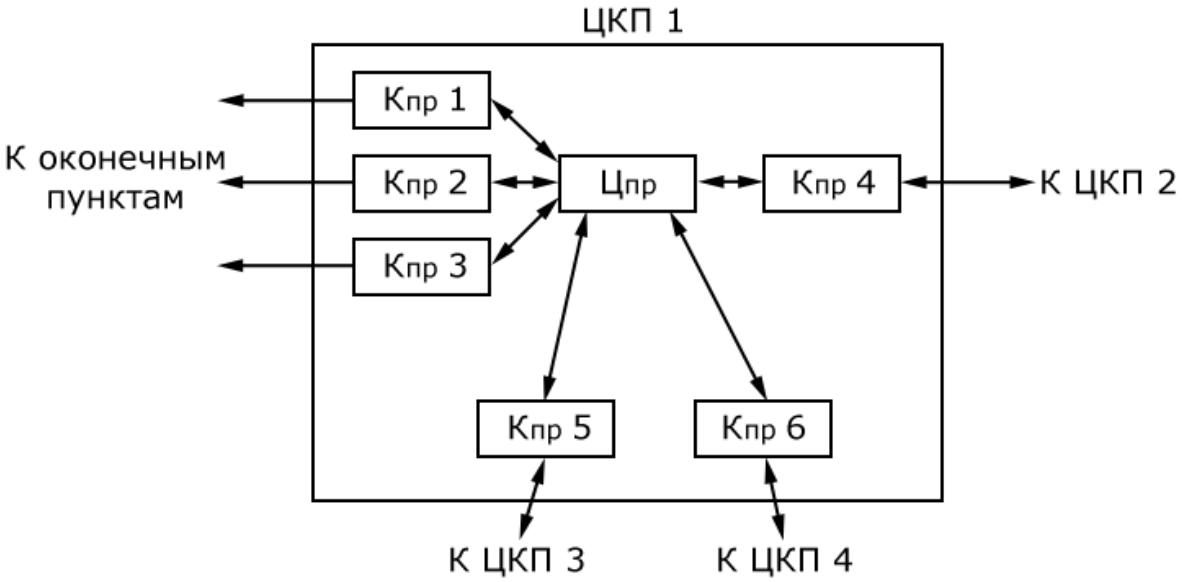
8.2. Программа P_2

В таблице 1 приведена таблица маршрутизации ЦКП по логическим канальным номерам LCN, которая получена в главе 7.

Таблица 1. Таблица маршрутизации ЦКП по логическим канальным номерам LCN

Номер канального процессора пакета, входящего в ЦКП	Номер канального процессора пакета, исходящего из ЦКП	LCN входящего пакета в ЦКП	LCN исходящего пакета из ЦКП	Признак использования Освн при формировании строки таблицы маршрутизации (да/нет)
4	5	220	193	да
4	5	3201	179	нет
5	4	179	3201	да
5	4	193	220	нет

Эта таблица составлена на примере структуры центра коммутации пакетов, приведенном на рис. 1.



1) Формирование первого пакета “Данные” (Д), находящегося в очереди принятых пакетов с канального процессора $К_{ПР}$=5.

На рис. 2 показано формат полей массива пакет “Данные” , поступившего с канального процессора $К_{ПР}$=5 и размещенного в первом массиве свободных блоков $О_{своб}$ с начальным адресом А(1).

Число байт	2	2	2	128

Начальный адрес А(1)	Первое адресное поле	Второе адресное поле	Заголовок пакета “Данные” (Д) – логический канальный номер LCN 12 бит (биты <1-8> 1 байта и биты <5-8> 2 байта), идентификатор пакета “Д” – (бит <1> 2 байта	Информационная часть

Рис. 2. Формат размещения пакета “Данные” (“Д”) в свободном блоке $О_{своб}$ с начальным адресом А(1)

Установим значение поля LCN этого пакета Д в биты <1-8> 1 байта и биты <5-8> 2 байта заголовка. В десятичном выражении LCN= 179.
Записать в информационную часть пакета значение *m* (исходные данные вариантов и контрольного примера приведены в разд. 8.6).
Перенести массив этого пакета в очередь массивов принятых пакетов $О_Д^{пм}$ (5) с канального процессора $К_{ПР}$=5 т.е. из очереди $О_{своб}$.
Откорректировать очередь свободных блоков $О_{своб.}$ На рис. 3 приведена характеристика этой очереди $Н_{своб.}$

$АН_{своб.}$

А(2)	А(N1)	N1-1

Рис.3. Характеристика $Н_{своб.}$

- установить характеристику очереди $Н_Д^{пм}$ (5) массивов принятых пакетов $О_Д^{пм}$ (5) с канального процессора $К_{ПР}$=5.
На рис. 4 приведена характеристика очереди $Н_Д^{пм}$ (5).

$АН_Д^{пм}$ (5)

А(1)	А(1)	1

Рис.4. Характеристика $Н_Д^{пм}$ (5)

2) Формирование второго пакета “Данные” (Д), находящегося в очереди принятых пакетов с канального процессора $К_{ПР}$=5.

Установим значение поля LCN этого пакета Д в биты <1-8> 1 байта и биты <5-8> 2 байта заголовка. В десятичном выражении LCN= 193.
Записать в информационную часть пакета значение *m*+1.
Перенести массив этого пакета в очередь массивов принятых пакетов $О_Д^{пм}$ (5) с канального процессора $К_{ПР}$=5 т.е. из очереди $О_{своб.}$.
Откорректировать $О_{своб.}$, $О_Д^{пм}$ (5), $Н_{своб.}$, $Н_Д^{пм}$ (5). На рис. 5 приведена характеристика этой очереди $Н_{своб.}$

$АН_{своб.}$

A(3)	A(N1)	N1-2

Рис.5. Характеристика $Н_{своб.}$

На рис. 6 приведена характеристика очереди $Н_Д^{ПМ}$ (5).

$АН_Д^{ПМ}$ (5)

A(1)	A(2)	2

D:=D+1
GO TO DISP8

8.3. Программа $Р_3$

1) Перенос первого пакета Д в очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=5) $О_Д^{ПМ}$ (5) в очередь пакетов на передачу в канальный процессор).
- определить номер строки таблицы маршрутизации для входящих пакетов с канального процессора 5 (табл. 1), в которой LCN входящего пакета в ЦКП совпадает с LCN в массиве пакета очереди $О_Д^{ПМ}$ (5) по адресу А(1). В данном примере LCN=179.
- заменяем LCN в массиве пакета по адресу А(1) на LCN исходящего пакета из ЦКП. В данном примере LCN=3201.
- снимаем этот массив пакета из $О_Д^{ПМ}$ (5) и устанавливаем в конец очереди на передачу из ЦКП в канальный процессор, номер которого определяется из определенной строки таблицы маршрутизации. В данном примере это в очередь $О^{ПД}$(4), т.е. в канальный процессор 4.
- производится коррекция очередей $О_Д^{ПМ}$ (5), $О^{ПД}$ (4) и характеристик $Н_Д^{ПМ}$ (5), $Н^{ПД}$ (4).

На рис. 7 приведена характеристика очереди $Н_Д^{ПМ}$ (5).

$АН_Д^{ПМ}$ (5)

A(2)	A(2)	1

На рис. 8 приведена характеристика очереди $Н^{ПД}$ (4).

А $Н^{ПД}$ (4)

A(1)	A(1)	1

2) Перенос пакета Д в очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=5) $О_{Д}^{ПМ}$ (5) в очередь пакетов на передачу в канальный процессор).

Эта операция производится самостоятельно аналогично приведенному выше переносу первого пакета.

Производится коррекция очередей $О_{Д}^{ПМ}$ (5), $О^{ПД}$ (4) и характеристик $Н_{Д}^{ПМ}$ (5), $Н^{ПД}$ (4).

На рис. 9 приведена характеристика очереди $Н^{ПД}$ (4).

А $Н^{ПД}$ (4)

A(1)	A(2)	2

D:=D+1
GO TO DISP8

8.4. Программа $Р_4$

Формирование двух пакетов “Данные” (Д), находящихся в очереди принятых пакетов с канального процессора $К_{ПР}$=4.

Эта операция производится самостоятельно на базе опыта, полученного при освоении программы $Р_2$. Записать в информационную часть первого и второго пакета соответственно значение *n* и *n*+1 (исходные данные *n* для вариантов и контрольного примера приведены в разд. 8.6).

На рис. 10 приведена характеристика очереди $Н_{Д}^{ПМ}$ (4).

А$Н_{Д}^{ПМ}$ (4)

A(3)	A(4)	2

D:=D+1
GO TO DISP8

8.5. Программа $Р_5$

Перенос пакетов Д из очереди массивов принятых пакетов (с канального процессора $К_{ПР}$=4) $О_{Д}^{ПМ}$ (4) в очередь пакетов на передачу в канальный процессор.

Эта операция производится самостоятельно на базе опыта, полученного при освоении программы $Р_3$.

На рис. 11 приведена характеристика очереди $Н^{ПД}$ (5).

А $Н^{ПД}$ (4)

A(3)	A(4)	2

```
D:=D+1
GO TO DISP8
```

8.6 Исходные данные для лабораторной работы

В таблице 2 приведены исходные данные пяти вариантов лабораторной работы и контрольного примера

Таблица 2. Исходные данные для лабораторной работы

Параметр	1 вариант	2 вариант	3 вариант	4 вариант	5 вариант	Контрольный вариант
N1	40	40	40	40	40	50
m	2	3	4	5	6	1
n	7	8	9	10	11	2

ГЛАВА 8. Сеть Frame Relay

8.1. Стек протоколов сети Frame Relay

Ретрансляция кадров FR (Frame Relay) – это технология сети передачи данных с пакетной коммутацией и так же как в сети стандарта X.25 использует технику виртуальных соединений. Сеть FR является усовершенствованной сетью пакетной коммутации стандарта X.25. Анализ процедур FR в настоящей главе проводится в сравнении с этой сетью. Технология FR, в основном, используется для объединения локальных сетей в рамках корпоративной сети связи. Сети FR используют на физическом уровне цифровые каналы связи, которые лучше по сравнению с аналоговыми каналами по показателю коэффициента ошибок BER. Стандарт сети X.25 разрабатывался с учетом использования аналоговых каналов связи. Это позволило упростить протоколы сети FR, что отразилось на использовании в транспортной сети при передачи данных только одного уровня (кроме физического). В стек протоколов FR при передаче данных входит только второй уровень, который фактически выполняет функцию сетевого уровня эталонной модели OSI, т.е. коммутацию блоков данных. В сети FR эти блоки данных называются кадрами (или фреймами). Искаженные в канале связи кадры FR сбрасываются без восстановления в транспортной части сети. Из канального уровня в сети FR осталась только одна функция, соответствующая модели OSI, – обнаружение с помощью контрольно-проверочной комбинации кадров, искаженных помехами в канале связи. Восстановление правильной последовательности принятых информационных кадров-фреймов (в сети X.25 они называются пакетами) возлагается в FR на протоколы верхних уровней оконечного пункта. Например, на протоколы сети Интернет. В качестве одного из возможных вариантов эта функция сквозного подтверждении («из конца в конец») может возлагаться на транспортный уровень оконечного оборудования. Эта разница в отсутствии подтверждения правильной последовательности на каждом канальном участке (между смежными узлами коммутации или между оконечным оборудованием и узлом коммутации) отражена и в названии сети - ретрансляции кадров (фреймов). В формате заголовка кадра FR отсутствует поле номера передаваемого кадра. Снятие функции подтверждения в транспортной части сети FR позволило повысить пропускную способность сети. На рис. 8.1 приведен стек протоколов FR.

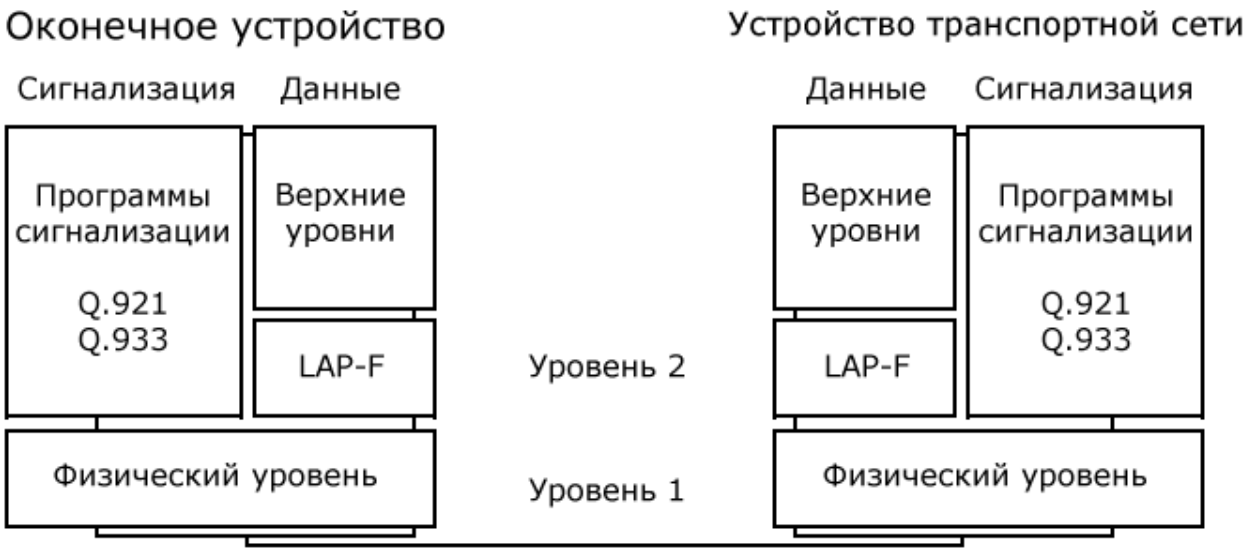


Рис. 8.1. Стек протоколов Frame Relay

Как видно из рисунка, стек протоколов сети FR зависит от выполняемой процедуры. В отличие от сети X.25 процедура сигнализации (установление и разъединение соединения по коммутируемому виртуальному каналу) выполняется в FR по выделенному виртуальному каналу. Эта процедура стандартизирована на канальном уровне стандартом ITU-T Q.921 и на сетевом уровне стандартом ITU-T Q.931. Протокол Q.921 выполняет функцию надежной доставки, аналогично канальному уровню сети X.25. Протокол Q.931 для установления КВК использует физические адреса конечных пунктов, которые задаются в формате, соответствующем рекомендации ITU-T E.164, который отличается от формата адресации в сети X.25 по рекомендации ITU-T X.121. Адрес согласно стандарту E.164 состоит из кода страны, национального кода адресата (т.е. адреса поставщика услуг) и номера абонента. Протокол маршрутизации для технологии FR не определен так же, как и для X.25. Поэтому используются фирменные протоколы производителя оборудования. Процедура передачи данных по виртуальному каналу в сети FR выполняется по протоколу LAP-F (Link Access Procedure for Frame mode bearer services) в соответствии с рекомендацией ITU-T Q.922. Приведем основные поля заголовка кадра данных по протоколу LAP-F.

- Идентификатор линии связи данных DLCI (Data Link Connection Identifier).

  В сети X.25 это поле называется логическим канальным номером LCN. Длина заголовка кадра FR составляет 2, 3 или 4 байта. При длине заголовка 3 или 4 байта длина DLCI соответственно 16 и 23 бита. При заголовке в 2 байта длина поля DLCI 10 бит, что позволяет использовать до 1024 виртуальных соединений по одному каналу связи, из которых используются 976, а остальные зарезервированы. При длине DLCI=23 бита используются DLCI в диапазоне от 131072 до 8126463.

Значение DLCI=0 применяется для установления и разъединения соединений;

- Поля DE, FEGN и BECN (по одному биту на каждый параметр)

применяются протоколом для управления трафиком и поддержания заданных пользователем требований трафика при установлении виртуального соединения. Сразу за заголовком следуют пересылаемые данные, длина которых не фиксированная (так же, как и в сети X.25). Аналогично сети X.25 в сети FR используется покадровая синхронизация с помощью флагов «01111110», а также контрольно-проверочная комбинация обнаружения искаженных в канале кадров с помощью циклического кода CRC.

8.2. Поддержка качества обслуживания

По запросу пользователя при установлении каждого виртуального соединения определяются несколько параметров трафика, связанных со скоростью передачи данных и влияющих на качество обслуживания QoS в части минимизации вероятности потерянных кадров.

- CIR (Committed Information Rate) – согласованная информационная скорость, с которой сеть будет передавать данные пользователя.
- Bc (Committed Burst Size) – согласованный объем информации, то есть максимальное количество бит, которое сеть будет передавать от этого пользователя за интервал времени T.
- Be (Excess Burst Size) – дополнительный объем информации, то есть максимальное количество бит, которое сеть будет пытаться передать сверх установленного значения Bc за интервал времени T.

Параметры QoS, связанные с задержками и вариациями задержек, стандартами Frame Relay, не оговариваются, так как изначально технология разрабатывалась только для передачи трафика данных, который не чувствителен к задержкам. *Интервал времени T* является согласованным интервалом измерения скорости передачи информации и вычисляется T=Bc/CIR.

Отсюда видно, что скорость CIR сеть должна гарантировано поддерживать при обычных условиях (CIR=Bc/T).

Например, если Bc=128 кбит, а CIR=64кбит/с, то T=2 сек. Для сети передачи данных характерен пульсирующий характер, который выражается отношением максимального потока данных к среднему за определенное время. Эта величина может достигать 100:1.

Можно задать значения CIR и T, тогда производной величиной станет величина всплеска трафика Bc. Основным параметром, по которому абонент и сеть заключают соглашение при установлении виртуального соединения, является согласованная скорость передачи данных. Для постоянных виртуальных каналов ПВК это соглашение является частью контракта на пользование услугами сети. При установлении коммутируемого виртуального канала соглашение об обслуживании заключается автоматически с помощью протокола Q.931 – требуемые параметры CIR, Bc и Be передаются в пакете запроса на установление соединения. Так как скорость передачи данных измеряется на каком-то интервале времени, то интервал T и является таким контрольным интервалом, на котором проверяются условия соглашения. В общем случае пользователь не должен за этот интервал передать в сеть данные со средней скоростью, превосходящей CIR. Если же он нарушает соглашение, то сеть не только не гарантирует доставку кадра, но помечает этот кадр признаком DE (Discard Eligibility), равным 1, то есть как кадр, подлежащий удалению. Однако кадры, отмеченные таким признаком, удаляются из сети только в том случае, если коммутаторы сети испытывают перегрузки. Если же перегрузок нет, то кадры с признаком DE=1 доставляются адресату. Такое щадящее поведение соответствует случаю, когда общее количество данных, переданных пользователем в сеть за период T, не превышает объема Bc+Be. Если же этот порог превышен, то кадр немедленно удаляется из сети. Рисунок 8.2 иллюстрирует случай, когда за интервал времени T в сеть по виртуальному каналу поступило 5 кадров. Средняя скорость поступления информации в сеть составила на этом интервале R бит/с и она оказалась выше CIR. Кадры F1,F2 и F3 доставили в сеть данные, суммарный объем которых не превысил порог Bc, поэтому эти кадры ушли дальше транзитом с признаком DE=0. Данные кадра F4, прибавленные к данным кадров F1,F2 и F3, уже превысили порог Bc, но еще не превысили порога Bc+Be, поэтому кадр F4 также ушел дальше, но уже с признаком DE=1. Он подлежит удалению только при перегрузке. Данные кадра F5, прибавленные к данным предыдущих кадров, превысили порог Bc+Be, поэтому этот кадр удаляется из сети, даже при отсутствии перегрузки.

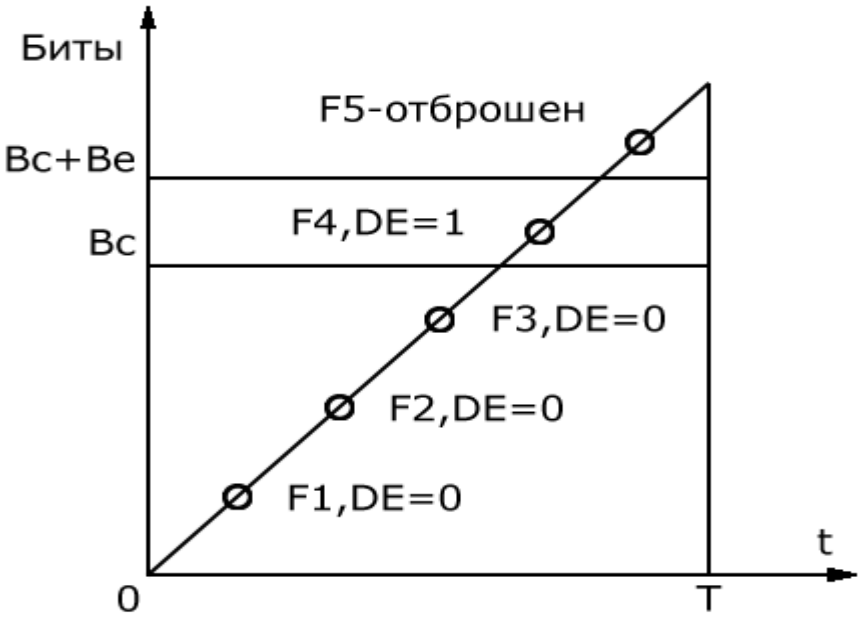


Рис. 8.2. Реакция сети на трафик пользователя

В технологии Frame Relay определен еще и дополнительный (необязательный) механизм управления кадрами. Это механизм оповещения конечных пользователей о том, что в коммутаторах сети возникли перегрузки (переполнение необработанными кадрами). Бит FECN (Forward Explicit Congestion Bit) кадра извещает об этом оконечное устройство принимающей стороны. На основании значения этого бита принимающая сторона должна с помощью протоколов более высоких уровней известить передающую сторону о том, что та должна снизить интенсивность отправки пакетов в сеть. Бит BECN (Backward Explicit Congestion Bit) извещает передающую сторону о перегрузке и является рекомендацией немедленно снизить темп передачи. В этом случае сетевое устройство (узел коммутации), возле которого возникла перегрузка, устанавливает в кадре бит BECN, а затем отправляет такой кадр узлам коммутации, которые стали причиной перегрузки. Эти узлы коммутации снижают поток кадров, поступающих в место перегрузки. Бит BECN обычно отрабатывается на уровне устройств доступа к сети. Frame Relay не требует от устройств, получивших кадры с установленными битами FECN и BECN, немедленного прекращения передачи кадров в данном направлении, как того требуют кадры RNR сетей X.25. Эти биты должны служить указанием снижения темпа передачи пакетов. Так как регулирование потока и принимающей и передающей сторонами инициируется в разных протоколах по-разному, то разработчики протоколов Frame Relay учли оба направления снабжения предупреждающей информацией о перегрузке в сети. В общем случае биты FECN и BECN могут игнорироваться. Но обычно

устройства доступа к сети FRAD (Frame Relay Access Device) отрабатывают, по крайней мере, признак BECN [15].

8.3. Типы виртуальных каналов в сети FR

Так же, как и в сети X.25, сеть FR поддерживает как *постоянные виртуальные каналы ПВК (PVC)*, так и *коммутируемые КВК (SVC)*. В таблице 8.1 приведены области предпочтительности каналов PVC и SVC. Как видно из таблицы выбор зависит от параметров трафика (интенсивность потоков и модель потоков) и топологии сети (уровня связности).

Таблица 8.1. Области предпочтительности каналов PVC и SVC

Параметры потоков или сети	Канал PVC	Канал SVC
Интенсивности потоков	От средних до высоких	Низкие
Модели потоков	Известные и повторяющиеся	Непредсказуемые и случайные
Уровень связности	Звездообразные и иерархические сети	Каждый с каждым

Интенсивность потока – это объем информации, передаваемой из одного узла в другой за единицу времени. Интенсивность измеряется количеством кадров, передаваемых за одну секунду. Использование каналов PVC предпочтительнее для потоков средней и высокой интенсивности, SVC – для низкой. Под моделями потоков подразумевается предсказуемость и частота сеансов передачи информации. Если два узла регулярно обмениваются информацией, то между ними следует установить канал PVC, позволяющий заранее определить соединение и полосу пропускания. Это позволяет не устанавливать соединение при каждом сеансе связи. Если же информация передается разным получателям, сеансы связи происходят от случая к случаю, передача информации прерывиста либо кратковременна, то следует использовать канал SVC. Применение в таких условиях каналов PVC означало бы установку соединений со всеми узлами, с которыми когда-нибудь, возможно, придется обмениваться информацией, и оплату бездействующих соединений. SVC - соединение с любым узлом устанавливается по мере надобности и оплачивается соответственно. Степень связанности соотносится с моделью потоков. Для наглядности будем полагать, что связность совпадает с моделью потоков. Для компании, которой требуется, главным образом, связь между центральным офисом и удаленными отделениями,

идеальной является звездообразная схема сети на основе каналов PVC. Каналы SVC хорошо работают в сетях, в которых может понадобиться установка связи между любой парой узлов. Это не означает, что любая полностью связная сеть должна строиться на каналах SVC. На рис. 8.3 представлена такая гибридная сеть на основе PVC и SVC. В отличие от сети X.25 в сети FR используется кроме ПВК и КВК третий тип виртуальных каналов – коммутируемый постоянный виртуальный канал КПВК (SPVC, Switched Permanent Virtual Circuit) . Его иногда называют программируемый постоянный виртуальный канал (Soft PVC). Для конечных устройств канал КПВК выглядит так же , как и канал ПВК, который устанавливается на абонентском участке (между пользователем и узлом коммутации). Между коммутаторами сети FR организуется КВК. Преимущество КПВК проявляется, когда возникают неисправности узла коммутации или каналов связи в транспортной части сети связи. В результате восстановление виртуального канала происходит значительно быстрее, чем в случае ПВК на всех участках виртуального канала (кроме абонентского участка).

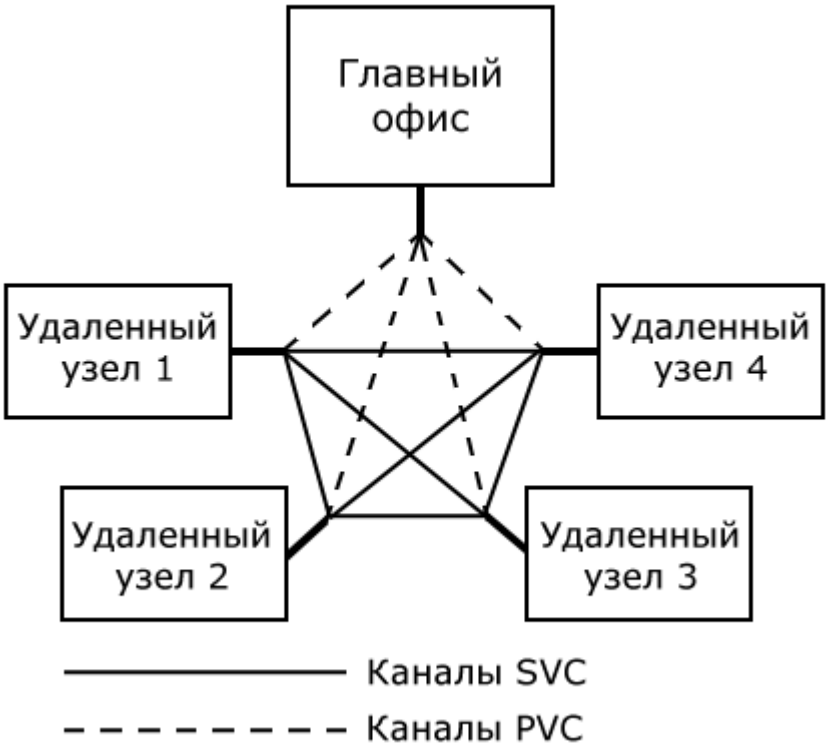


Рис. 8.3. Гибридная сеть на основе каналов PVC и SVC

На рис. 8.4 проиллюстрирован принцип работы КПВК.

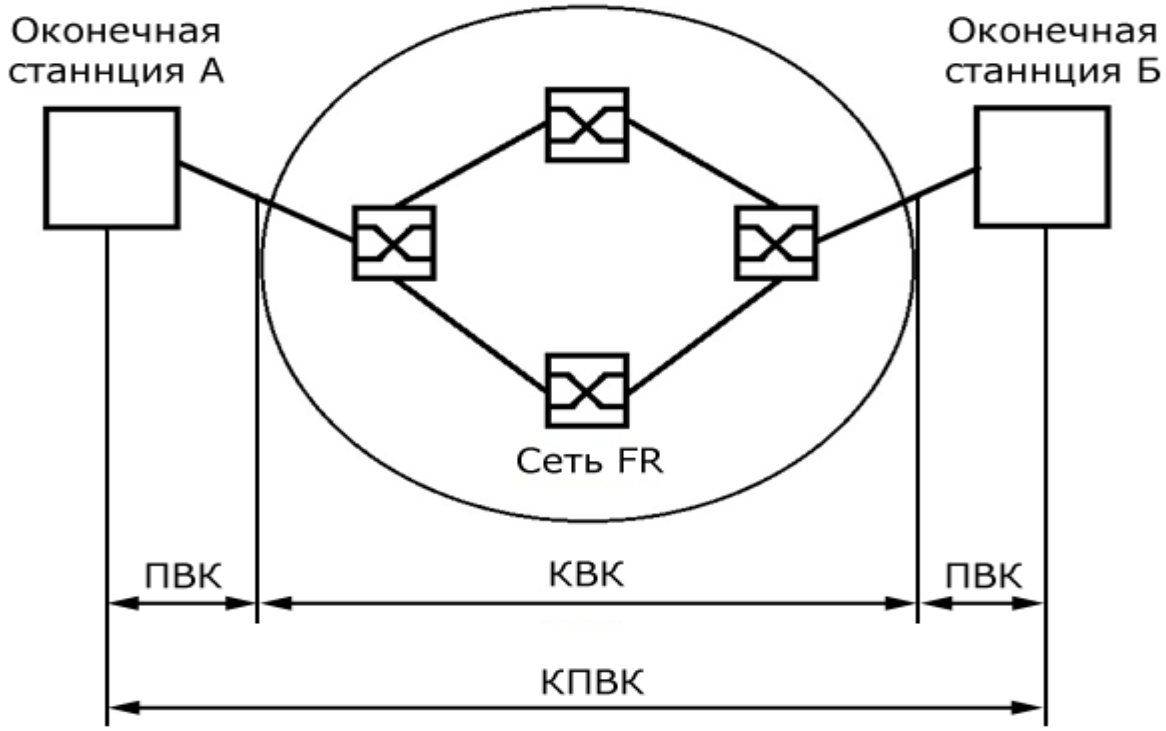


Рис. 8.4. Принцип работы КПВК

В сети FR в отличие от X.25 предусмотрена процедура контроля каналов PVC. Для этих операций определены два сообщение: STATUS ENQUIRY (запрос состояния) и STATUS (состояние). Пользователь отправляет в сеть сообщение STATUS ENQUIRY, чтобы запросить информацию о состоянии PVC соединений. Сеть возвращает сообщение STATUS, содержащее информацию обо всех PVC в канале связи.

8.4. Установление коммутируемого виртуального канала

Как видно из рис. 8.1 стек протоколов по установлению и разъединению коммутируемого виртуального канала состоит из двух уровней (кроме физического), которые выполняют функции второго и третьего уровня модели OSI по переносу сообщений сигнализации. Канальный уровень сети FR LAP-D определенный в рекомендациях ITU-T Q.921, принадлежит к тому же семейству протоколов HDLC, что и протокол LAP-B второго уровня сети X.25. Основная задача состоит в безошибочном переносе сигнальных сообщений третьего уровня сети FR. Третий уровень, определенный в рекомендации ITU-T Q.931 включает функции по установлению и разъединению коммутируемого виртуального канала. В отличие от сети X.25 при установлении коммутируемого виртуального канала в сети FR

необходимо определить может ли сеть обеспечить затребованные пользователем показатели качества обслуживания QoS (CIR, Bc и Be). Рис. 8.5 иллюстрирует процесс установления коммутируемого виртуального канала между двумя пользователями. Все управляющие сообщения по установлению КВК передаются по общему виртуальному каналу сигнализации, для которого на интерфейсе пользователь сети выделен логический номер DLCI=0. Это соответствует тому, что процедура сигнализации в сети FR осуществляется по выделенному каналу в отличие от X.25.

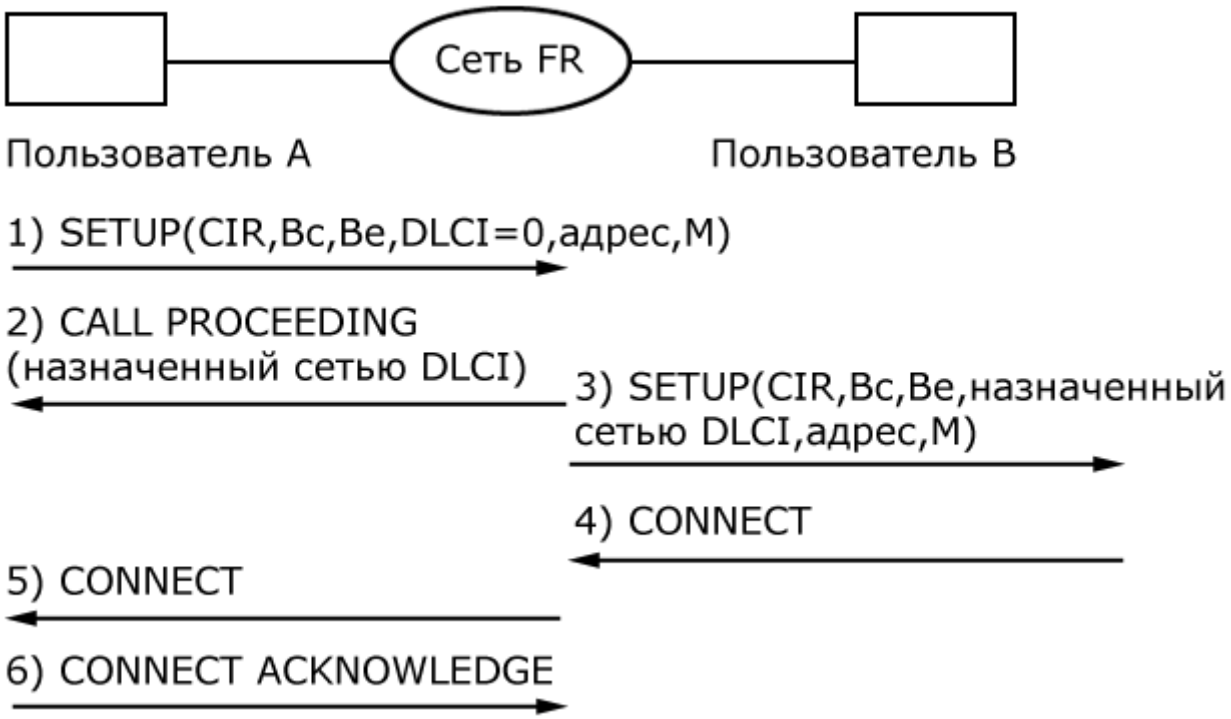


Рис. 8.5. Диаграмма установления коммутируемого виртуального канал

Опишем процесс установления КВК.

- Пользователь A посылает сообщение запроса на установление КВК. В сети FR это сообщение называется SETUP (“установка параметров”). Сообщение SETUP указывает желаемые пользователем параметры, физические адреса отправителя и получателя (в соответствии с рекомендациями ITU-T E.164), а также максимальный размер кадра M). Параметр DLCI, относящийся к устанавливаемому соединению, не обязателен.
- Сообщение CALL PROCEEDING (подтверждение вызова) получает от сети

вызывающий пользователь. Это сообщение содержит параметр номера логического канала DLCI, назначенный сетью для устанавливаемого КВК (если этот параметр отсутствовал в сообщении 1).

- Сообщение SETUP, которое поступает пользователю В, кроме параметров сообщения 1 содержит параметр назначенный сетью логический номер канала DLCI.
- Сообщение CONNECT (подтверждает соединение) информирует через сеть вызывающего абонента об успешном соединении.
- Повтор п.4.
- Сообщение CONNECT ACKNOWLEDGE (подтверждение приёма) подтверждает приём вызывающим абонентом сообщения CONNECT. Переход в фазу передачи данных по установленному КВК.

8.5. Виртуальная частная сеть на основе сети Frame Relay

Услуга виртуальных частных сетей VPN является одной из основных услуг, которую предоставляет сеть FR, а также и другие технологии сетей (подлежащие рассмотрению в следующих главах). Виртуальная частная сеть в определенной степени воспроизводит свойства реальной частной сети, когда оборудование и каналы связи находятся в собственности владельца сети. VPN использует оборудование связи, которым владеет оператор публичной сети. Цель технологий VPN состоит в максимальной обособленности отдельных групп пользователей этой публичной сети. Технология VPN предназначена для выполнения двух задач. Одна из них заключается в обеспечении информационной безопасности в части защиты от несанкционированного доступа к пользователям такой виртуальной сетью. В качестве способов защиты от несанкционированного доступа понимается обеспечение конфиденциальности и целостности сообщений в сети, доступа к предоставляемым услугам связи и др. Другая задача VPN состоит в качестве обслуживания QoS пользователей связью. С помощью сети провайдера общего пользования может быть организовано много виртуальных частных сетей VPN, каждая из которых служит для определенной группы пользователей. Для построения VPN на базе сети FR используются постоянные виртуальные каналы PVC или программируемые постоянные каналы SPVC. На рис. 8.6 приведена логическая структура двух VPN-сетей (А и В) на основе стандарта Frame Relay. На рисунке не показаны коммутаторы FR.

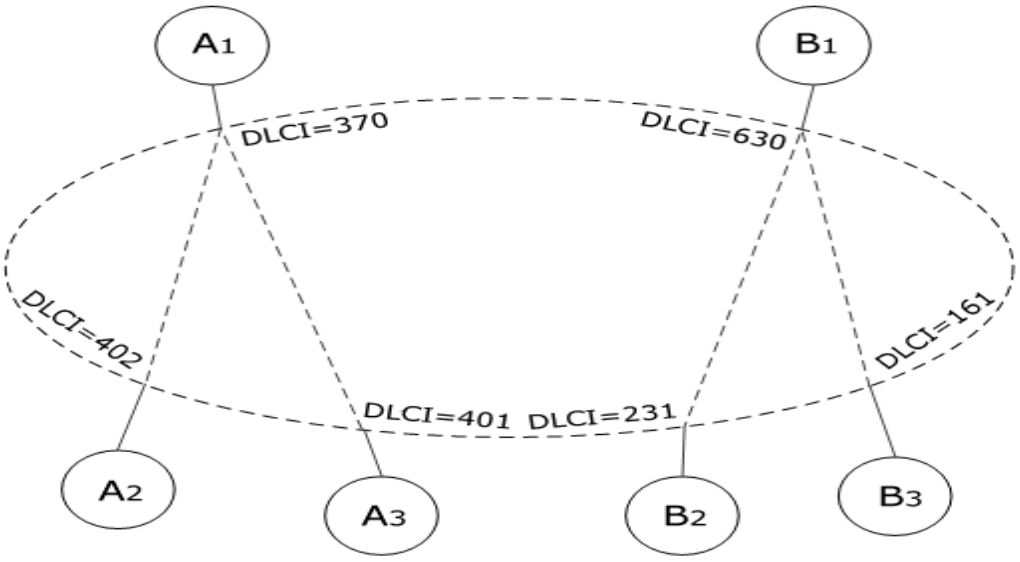


Рис. 8.6. Логическая структура VPN-сетей Frame Relay

Первая VPN A пользователей центрального офиса A_1 и двух его филиалов – A_2 и A_3. FR предоставляет виртуальные каналы между главным офисом и филиалами с номерами идентификаторов DLCI =370, 402, 401 (созданных в оконечных коммутаторах FR с соответствующими офисами A_1, A_2, A_3). Аналогично вторая VPN B включает пользователей центрального офиса B_2 и двух его филиалов – B_2 и B_3. FR предоставляет виртуальные каналы между главным офисом и филиалами с номерами идентификаторов DLCI =630, 231, 161 (созданных в оконечных коммутаторах FR с соответствующими офисами B_1, B_2, B_3). Пользователи каждой VPN получают по виртуальным каналам доступ только к пользователям своей VPN.

8.6. Стандарт ITU-T G.1000 (SLA)

Одной из сложных задач по обеспечению гарантированного обслуживания SLA является выбор характеристик качества обслуживания и их параметров. Для решения этой задачи при заключении соглашения SLA в соответствии с рекомендацией ITU-T G.1000 [16, 17] предлагается производить опрос пользователей с последующей статистической обработкой мнений. Эта рекомендация содержит таблицу в виде матрицы (рис. 8.7) для определения различных компонентов качества обслуживания.

Функции услуги		Скорость	Точность	Доступность	Надежность	Безопасность	Простота	Гибкость
		I	II	III	IV	V	VI	VII
Заключение контракта 1								
Управление услугой	Поставка, предоставление услуги 2							
	Изменение 3						X	
	Поддержка услуги 4							
	Ремонт и восстановления 5		X					
	Прекращение обслуживания 6							
Техническое качество вызова	Установление соединения 7							
	Передача информации 8					X		
	Разрыв соединения 9							
Денежные расчеты 10						X		
Управление сетью/услугой со стороны пользователя 11								

Рис. 8.7. Матрица для сбора требований к уровню услуг со стороны пользователя

В таблице по горизонтали расположены 7 критериев качества услуг: скорость, точность доступность, надежность, безопасность, простота, гибкость. Обращает на себя внимание среди этих критериев показатель безопасности. Успешное проведение работ в обеспечении ИБ позволит операторам получить преимущества в конкуренции. По вертикали матрицы расположены 11 функций обслуживания:

1. заключение контракта;
2. поставка и предоставление услуги;
3. изменение услуги;
4. поддержка услуги;
5. ремонт и восстановление;
6. прекращение обслуживания (пункты 1-6 образуют группу «управление службой»);
7. установление соединения;
8. передача информации;
9. разрыв соединения (пункты 7-9 образуют группу «качество соединения»);
10. денежные расчеты;
11. управление сетью/службой со стороны пользователя.

Ниже приведено краткое содержание всех наименований матрицы по вертикали и

горизонтали.

По вертикали.

- Заключение контракта: все мероприятия, начиная с момента установления связи между поставщиком услуги и пользователем до момента подписания контракта.
- Поставка, предоставление услуги: все мероприятия, связанные с предоставлением услуги, начиная с момента вступления контракта в силу и до момента, когда пользователь получает возможность воспользоваться услугой.
- Изменение: все мероприятия, связанные с изменениями в услугах, начиная с запроса пользователя на изменение и до момента реализации изменений.
- Поддержка услуги: все мероприятия, связанные с поддержкой услуг, с тем, чтобы обеспечить пользователю удобный доступ к услуге.
- Ремонт и восстановление: все мероприятия, связанные с восстановлением услуг после неисправностей, приведших к частичной или полной потере для пользователя пользования услугами.
- Прекращение обслуживания: все мероприятия, связанные с прекращением предоставления услуг, начиная с момента запроса на них пользователем и до момента их полного использования.
- Установление соединения: все мероприятия, связанные с действием услуг, начиная с момента запроса на них пользователем и до момента получения ответа.
- Передача информации: все мероприятия, начиная с момента установления соединения и до момента разрыва соединения любой из сторон.
- 9Разрыв соединения: все мероприятия, связанные с запросом на разрыв установленного соединения и до момента восстановления системы для последующего использования.
- Денежные расчеты: все мероприятия, связанные с оплатой и расчетами за оказанные пользователю услуги.
- Управление сетью/службой со стороны пользователя: все мероприятия, связанные с отслеживанием пользователем предварительно согласованных изменений в услугах.

По горизонтали.

- Скорость: быстрота, с которой исполняются функции услуг, например, скорость, с которой услуга предоставляются клиенту – готовность.

- Точность: четкость и полнота исполнения функции услуг по отношению к эталонному уровню.
- Доступность: четкость и полнота, с которой в момент запроса может быть установлен доступ пользователя к функциям услуги.
- Надежность: вероятность того, что функция услуг будет исполняться в рамках установленных ограничений по скорости, точность и доступности в течение одного года.
- Безопасность: конфиденциальность, в соответствии с которой поставщик услуг будет выполнять функции услуг в соответствии с контрактом.
- Простота: легкость применения функций услуг (высокое качество обслуживания).
- Гибкость: возможность предоставления пользователям функций услуг по особым запросам.

Таблица задумана как шаблон для сбора сведений о QoS для любой услуги. Для облегчения пользования таблицей и получения более однородных ответов ниже приведено краткое описание рекомендуемого содержания некоторых ячеек матрицы. Из приведенного выше содержания матрицы по горизонтали и вертикали следует, что характеристики SLA охватывают весь процесс связи, начиная с заключения контракта и кончая штрафами при эксплуатации. Матрица для сбора требований к качеству обслуживания со стороны пользователя разработана в качестве шаблона. Для обеспечения однородности в рекомендации ITU-T G.1000 приведено содержание ячеек матрицы (т.е. на пересечении горизонтали и вертикали таблицы). Например, ячейка 8-V соответствует характеристике качества передачи информации в части критерия безопасность. В рекомендации ITU-T G.1000 эта ячейка характеризует требования пользователя к конфиденциальности информации во время ее передачи. Ячейка 10-V содержит требования о защите от угроз безопасности операций по расчетам между оператором/провайдером и пользователем. Ячейка 3-VI характеризует легкость и удобство внесения поставщиком услуг изменений, вносимых в услугу. Ячейка 5-II характеризует правильности и полноту устранения неисправности.

8.7. Соглашение об уровне обслуживания сети Frame Relay

Для службы передачи данных сетей связи более современных технологий (например, сети ATM) в качестве основного показателя обслуживания пользователей принято значение вероятности потерь информационных блоков данных. В сетях передачи данных Frame Relay,

так же как и в сети X.25 международными организациями по стандартизации не предусмотрено выполнение требований пользователей по этому показателю качества обслуживания. В то же время международной организацией ITU-T разработан стандарт E.860, в котором определено качество обслуживания как «степень соответствия качества, предоставляемого пользователю поставщиком услуг, по согласованию между ними». Этот документ был разработан в 2002 году, т.е. значительно позже появления в эксплуатации сетей Frame Relay и X.25. Тем не менее, на этапе начала эксплуатации сетей FR международный Форум Frame Relay разработал в 1999 году положения для сети FR о гарантии провайдером некоторых параметров качества обслуживания [15]. Эти положения явились первым опытом, который послужил в дальнейшем более глубокой проработки для других сетей связи положений о письменном соглашении (контракте) об уровне обслуживания *SLA (Service Level Agreements)*. Составление SLA предусматривает согласование компенсаций (штрафы) пользователю сети при невыполнении гарантий поставщиком. Возможны разнообразные формы этих компенсаций. Для этой цели предусматриваются определенные средства мониторинга. Ниже приведем те показатели SLA, которые подлежали согласованию для сетей FR.

Коэффициент доставки (вероятность потери) кадров

В условиях перегрузки в сети Frame Relay пакеты могут удаляться, поэтому в соглашении SLA оговариваются гарантии их доставки. Соответствующий параметр соглашения называется вероятность потерь кадров/пакетов (*FDR – Frame/packet Delivery Ratio*). Надо отметить, что провайдеры, как правило, различают пакеты, отправленные с соблюдением заданных значений CIR и с превышением этих значений (с установленным битом DE). Обычно провайдеры предлагают коэффициент FDR около 99,9x% CIR FDR для кадров, не подлежащих удалению, и 9x% DE FDR для кадров с установленным битом DE. FDR рассчитывается по формуле: CIR FDR = (количество доставленных кадров CIR – исключения)/(количество отправленных кадров CIR - исключения) DE FDR = (число доставленных кадров DE – исключения)/(число отправленных кадров DE - исключения). Под исключениями принимаются потери кадров из-за повреждений средств локального доступа, а также вследствие плановых остановов сети провайдером.

Доступность сети (коэффициент готовности сети)

Одним из наиболее важных параметров в соглашениях SLA – это доступность сети. Доступность сети определяет время, в течение которого можно пользоваться сетью. Соглашение SLA обычно гарантирует доступность от 99,95% до 100% при расчетном периоде в один месяц. Обычно для расчета используется следующая формула: (24 часа *

количество дней в месяце * количество узлов сети - время простоя сети – исключенное время)/(24 часа * количество дней в месяце * количество узлов сети – исключенное время).

Простои в сети характеризуются такими параметрами. - Перерывы в обслуживании. - Потери данных, превышающие согласованные уровни. - Задержка в сети, превышающие согласованные уровни. Длительность простоя измеряется от момента обнаружения нарушения до момента восстановления обычной работы. В таблице 8.2 перечислены компоненты службы Frame Relay, учитываемые и не учитываемые при определении времени простоя.

Таблица 8.2. Компоненты, которые учитываются и не учитываются при определении времени простоя

Учитываемые компоненты	Не учитываемые компоненты
Все компоненты службы Frame Relay, предоставляемые и управляемые провайдером. Оборудование, предоставляемое провайдером и установленное у клиента CPE.	Неисправность любого компонента, средств доступа и оборудования CPE, не предоставленного провайдером. Отключение сети для проведения плановых работ. Простои вследствие обстоятельств, которые провайдер не имел возможности предотвратить.

CPE (Customer Provider Equipment) – оборудование, установленное у клиента (в офисе, на предприятии, дома): маршрутизаторы, учрежденческая АТС, автоответчик, устройство для подключения цифровой линии от провайдера и др.

Доступность каналов PVC (коэффициент готовности PVC)

Многих пользователей интересует не только доступность сети в целом, но и доступность отдельных каналов PVC. Включение в соглашение SLA соответствующего пункта позволяет обеспечить нужные параметры связи между отдельными узлами или для потоков определенных форматов. Доступность канала PVC Frame Relay «из точки в точку» определяется как отношение времени, в течение которого этот канал способен передавать данные, ко времени проведения измерений. Доступность канала в течение месяца рассчитывается по следующей формуле: (24 часа * количество дней в месяце – время простоя PVC – исключенное время)/(24 часа * количество дней в месяце – исключенное время) В табл. 8.3 приведены компоненты канала PVC, которые учитываются и не учитываются при нахождении времени простоя.

Таблица 8.3. Компоненты, которые учитываются и не учитываются при определении времени простоя

Учитывается	Не учитывается
Каждый канал (в отдельности).	Неисправность любого компонента по другую сторону линии раздела. Отключение сети для проведения плановых работ. Простои вследствие обстоятельств, которые провайдер не имел возможности предотвратить.

Реальная польза от показателя доступности каналов PVC состоит в возможности ее регулирования в зависимости от потоков, проходящих по каналам. Каналам с менее важными потоками назначается низкая доступность, что позволяет достичь определенной экономии.

Задержка в канале PVC

Для пользователя важны не только доступность сети и ее компонентов, но и скорость передачи данных. Во многих соглашениях SLA Frame Relay имеется пункт о задержках в сети. Для потоков, чувствительных к задержкам, минимизация этого параметра очень важна. Задержка в канале PVC определяется как время, необходимое кадру для прохождения по каналу «из точки в точку» и обратно (часто это называется задержкой с подтверждением приема). Измерение может проводиться от точки к точке, между линиями раздела, с учетом средств локального доступа. Возможны измерения между коммутаторами, в пределах сети провайдера. Некоторые провайдеры усредняют задержку за день, неделю или месяц, указывая в соглашении минимальное значение. В таблице 8.4 приведены примеры составляющей задержки.

Таблица 8.4. Примеры составляющей задержки пакетов

Примеры	От коммутатора к коммутатору	От точки к точке («от конца в конец»)
По стране	Порт 64 Кбит/с=130мс	Порт 64 Кбит/с=200мс
Между странами	Порт 64 Кбит/с=160мс	Порт 64 Кбит/с =250мс

В число показателей качества обслуживания QoS значение задержки не входит в стандартах протоколов FR. Тем не менее, многие производители поддерживают передачу речи по сети FR. Уменьшение задержек достигается за счет приоритезации речевого трафика и использования достаточно больших скоростей передачи на магистральных линиях связи. Для уменьшения задержек на низкоскоростных каналах связи применяется уменьшение максимального размера кадров неречевого трафика (фрагментация). Это позволяет избежать задержек, связанных с нахождением в очереди на передачу очень длинных кадров в целях уменьшения задержки. Обратим внимание, как было отмечено выше, в состав сообщения SETUP при установлении коммутируемого виртуального канала входит параметр максимального размера кадра в данном виртуальном соединении. Отметим, что согласно стандарту максимальный размер поля данных кадра FR составляет 4056 байт. Для передачи речи по сетям FR разработаны соответствующие стандарты, в частности, стандарты форума Frame Relay.

8.8. Особенности сети Frame Relay по сравнению с сетью X.25

Перечислим на основании приведенного выше материала особенности сети FR по сравнению с сетью X.25.

- Стандартом на сеть FR предусмотрено согласование с провайдером при установлении соединения требований пользователя к показателям трафика, влияющим на качество обслуживания QoS. Сеть X.25 такую возможность пользователю не предоставляет.
- Стек протоколов транспортной сети FR состоит из двух уровней (физический и канальный). Стек протоколов транспортной сети X.25 состоит из трех уровней, соответствующих модели OSI. Искаженные в канале кадры FR не восстанавливаются в транспортной сети FR. Канальный уровень FR выполняет процедуры обнаружения искаженных кадров на приеме и коммутацию кадров “Данные”. В сети X.25 процедуры канального уровня обнаруживают искаженные информационные кадры и восстанавливают их путем повтора из буфера. На сетевом уровне X.25 производится

коммутация информационных кадров.

- В сети FR установление и разъединение коммутируемого виртуального канала осуществляется по выделенному виртуальному каналу. В сети X.25 функции установления и разъединения КВК выполняются в том же виртуальном канале, в котором производится обмен пакетов “Данные”.
- В формате кадра FR предусмотрены поля оповещения конечных пользователей конкретных виртуальных каналов о перегрузке. В сети X.25 предусмотрено оповещение о перегрузке относительно всех пользователей, подключённых к центру коммутации.
- В сети FR производители поддерживают не только службу передачи данных, как и в X.25, но и службу передачи речи. Следует отметить, что служба передачи речи в FR не стандартизирована международной организацией. В сети X.25 службы передачи речи нет.
- В сети FR кроме постоянного и коммутируемого виртуального канала предусмотрен третий тип виртуального канала - коммутируемый постоянный виртуальный канал КПВК (SPVC).
- В сети FR в отличие от X.25 предусмотрена процедура контроля постоянного виртуального канала.
- В VPN на базе FR в отличие от закрытой группы абонентов на базе X.25 предусмотрена возможность выполнения требований пользователей по согласованию показателей трафика с провайдером.
- Для сети FR предоставлена возможность гарантировать обслуживание пользователей, заключив для этого соглашение об уровне обслуживания SLA с провайдером сети. Международная организация Форум Frame Relay для этой цели разработала специальный документ.

  Для пользователей сетью X.25 такая возможность не предоставлена.

ГЛАВА 9. Сеть АТМ. Физический уровень

9.1. Основные положения и стек уровней сети АТМ

Сеть АТМ (асинхронный метод передачи, Asynchronous Transfer Mode) так же, как и X.25 и Frame Relay является сетью пакетной коммутации [18,19]. Сеть АТМ можно рассматривать как развитие сети Frame Relay. В отличие от FR сеть АТМ с самого начала создавалась как мультимедийная универсальная технология для передачи всех видов информации (данные, речь, видео и др.). В технологии АТМ для этого заложены механизмы, позволяющие эффективно передавать такой разнородный трафик. АТМ обеспечивает интегрированную передачу данных, речи, подвижных и неподвижных изображений методом мультиплексирования в едином цифровом тракте. Обеспечение передачи высококачественной речи и изображений означает, что сквозные («из конца в конец») задержки в территориально разнесенных сетях не должны превышать нескольких десятков миллисекунд. Примерами использования технологии АТМ является сеть транспортной системы метро Москвы, сеть департамента города Москвы по образованию. АТМ является так же, как и сеть FR технологией с ретрансляцией кадров, которые в сети АТМ называются ячейками. В отличие от FR и X.25, в которых кадры и пакеты могут иметь любой размер вплоть до некоторого максимума, все ячейки АТМ имеют одну и ту же строго определенную длину – 53 байта. Из 53 байтов 5 является заголовком ячейки, а оставшиеся 48 используются для передачи пользовательских данных (которые могут включать служебную и другую информацию в зависимости от типа трафика). Ограничение ячейки фиксированной длиной упрощает реализацию некоторых процедур технологии АТМ аппаратным способом. Специализированные высокоскоростные наборы микросхем уменьшают задержки простаивания данных в очереди на обработку в коммутаторах. Поэтому при прохождении через сеть АТМ трафик реального времени не имеет больших задержек «из конца в конец». Это сочетание фиксированного размера ячейки АТМ и реализации многих процедур высокоскоростным аппаратным способом дает технологии АТМ возможность объединить все типы трафика в одной высокоэффективной коммутирующей платформе. В сети АТМ так же, как и в сети FR стек протоколов определяется конкретной процедурой сигнализации или передачей трафика т.к. сигнализация является выделенной. На рис. 9.1 показано из каких уровней состоит архитектура АТМ. Уровни АТМ, так же, как и FR, соответствуют уровням 1 и 2 эталонной модели OSI. Искаженные в канале ячейки не восстанавливаются в транспортной сети.

Рис. 9.1. Уровни ATM

9.2. Физический уровень ATM

Как показано на рис. 9.1 физический уровень ATM состоит из двух подуровней: подуровня конвергенции TC (Transmission Convergence) и подуровня физической передающей среды PM (Physical Medium).

9.2.1. Подуровень физического уровня ATM «Конвергенция передачи»

Для исходящей передачи подуровень конвергенции TC (Transmission Capabilities) принимает ячейки от уровня ATM, формирует их в поток данных и передает его подуровню физического носителя. Из 53 байт ячейки 48 байт являются информационными, а 5 байт включают данные заголовка ячейки. В состав заголовка включены поля логических номеров виртуальных каналов. Последний байт заголовка служит контрольно-проверочной комбинацией КПК остальной части заголовка ячейки. Этот КПК циклического кода (полином x^8+x^2+x+1), которые обычно применяются в ATM, позволяет исправлять одиночные ошибки, обнаруживать все двойные ошибки и большинство ошибок большей кратности. В оптоволоконных системах связи одиночные ошибки составляют более 95%. В следующих главах будет подробно рассматриваться исправляющая способность кодов. При приеме ячейки от уровня ATM подуровень TC формирует этот байт КПК. Поле КПК в ATM называется *контролем ошибок в заголовке HEC (Header Error Check)*. При приеме ячеек с канала подуровень TC проверяет значение HEC, чтобы убедиться в корректности принятой ячейки. Ячейки ATM сбрасываются при невозможности исправить ошибки в заголовке. HEC выполняет функцию предотвращения неправильной маршрутизации ячейки. Подуровень TC выполняет также функцию синхронизации ячеек, т.е. определение границы ячейки. Эта процедура основана на проверке соответствия HEC остальным четырем байтам заголовка. В

отсутствии пользовательского трафика в канал передаются пустые ячейки, а не флаги 01111110 как в случае FR и X.25. Такой кадр-асинхронный режим передачи и является причиной названия ATM (Asynchronous Transfer Mode) асинхронным методом передачи.

9.2.2. Подуровень физической передающей среды ATM на базе PDH

Подуровень физической передающей среды *PM (Physical Medium)* выполняет функцию скремблирования, а также отвечает за передачу и прием скоростей электрического и оптического сигнала. Напомним, что под скремблированием понимается процедура перемешивания потока данных с целью улучшения поимпульсной синхронизации, т.е. определения середины каждого принимающего бита. Кроме синхронизации скремблирование служит также в некоторой степени защитой от прослушивания трафика. Используются две стандартизированные ITU-T технологии транспортных средств первичной сети связи для передачи ячеек ATM: *синхронная цифровая иерархия SDH (Synchronous Digital Hierarchy)* и *плезиохронная цифровая иерархия PDH (Plesiochronous Digital Hierarchy)*. Параметры этих систем рассмотрены в рекомендациях ITU-T серии G.7xx. Система передачи синхронной оптической сети SONET (Synchronous Optical Network), используемая в США, по своим принципам мало отличается от системы SDH, принятой в Европе. Иерархия строится на основе основного цифрового канала (ОЦК) 64 кбит/с. На рис. 9.2 показан формат размещения ячеек ATM в кадре иерархического уровня скоростей E3 (см. глава 3, таблица 3.1).

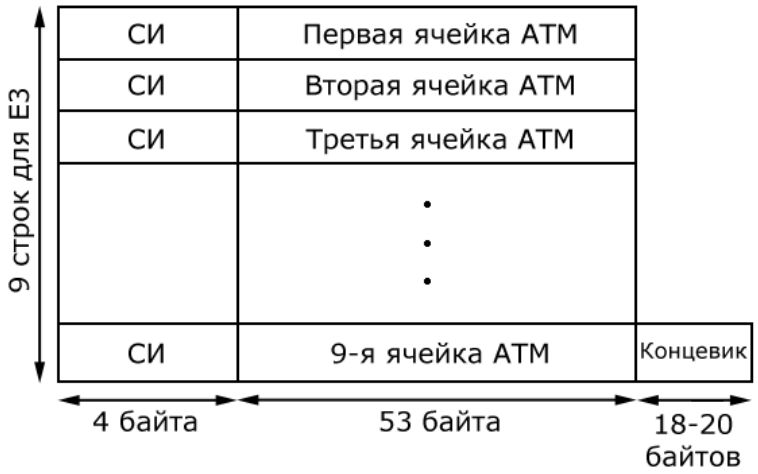


Рис. 9.2. Размещение ATM-ячеек в кадре иерархического уровня скоростей E3 с использованием протокола PLCP

Такое преобразование выполняет протокол PLCP (Physical Layer Convergence Protocol). Передача кадра занимает 125 мкс для полезной нагрузки данных в E3. Концевик кадра состоит из 18-20 байтов и содержит информацию для синхронизации с кадром E3.

Примечание: СИ – служебная информация

9.2.2.1. Недостатки PDH

Технология плезиохронной цифровой иерархии PDH (глава 3) обладает недостатками, основным из которых является сложность и неэффективность операций мультиплексирования и демультиплексирования пользовательских данных [20]. Сам термин «плезиохронный», то есть «почти синхронный», используемый для этой технологии, говорит о причине такого явления — отсутствии полной синхронности потоков данных при объединении низкоскоростных каналов в высокоскоростные. Асинхронный подход к передаче кадров потребовал в PDH произвоить вставку бита или нескольких битов для синхронизации между кадрами. В результате для извлечения пользовательских данных из объединенного канала необходимо полностью демультиплексировать кадры объединенного канала. Например, чтобы получить данные одного абонентского канала 64 Кбит/с из кадров канала E3 необходимо произвести демультиплексирование этих кадров до уровня кадров E2, затем — до уровня кадров E1, а в конце концов демультиплексировать и сами кадры E1. Если PDH используется в сети только в качестве транзитной магистрали между крупными узлами, то операции мультиплексирования и демультиплексирования выполняются исключительно в конечных узлах, и проблем не возникает. Но если необходимо выделить один или несколько абонентских каналов в промежуточном узле сети PDH, то эта задача простого решения не имеет. Как вариант предлагается установка двух мультиплексоров уровня E3 и выше в каждом узле сети. Первый выполняет полное демультиплексирование потока и отвод части низкоскоростных каналов абонентам, а второй опять собирает в выходной высокоскоростной поток оставшиеся каналы вместе с вновь вводимыми. При этом количество работающего оборудования увеличивается.

Еще одним недостатком технологии PDH является отсутствие встроенных средств сетевого управления. Современные сети связи требуют организации комплексного сетевого управления, которое включало бы решение как задач автоматизации технической эксплуатации систем связи, так и задач управления услугами, контроля качества услуг и др. Для решения поставленной задачи ITU-T предлагает использовать концепцию TMN (Telecommunications Management Network, сеть управления электросвязью) [21]. TMN есть специализированная сеть обеспечивающая управление сетями электросвязи и их услугами путем организации взаимосвязи с компонентами различных сетей электросвязи на основе единых интерфейсов и протоколов, стандартизированных ITU-T. В настоящее время в большей части зарубежных сетей связи достаточно полно реализовано управление

устройствами и элементами оборудования связи.

Отметим еще один недостаток технологии PDH. Это относится к слишком низким по современным понятиям скоростям передачи данных. Волоконно-оптические кабели позволяют передавать данные со скоростями до нескольких терабит в секунду, что обеспечивает объединение в одном кабеле тысячи и миллионы пользовательских каналов, но эту возможность технология PDH не реализует - ее иерархия скоростей заканчивается уровнем E4 со скоростью 139,264 Мбит/с.

9.2.3. Подуровень физической передающей среды ATM на базе SDH

Указанные выше недостатки PDH были учтены и преодолены разработчиками технологий *SDH (Synchronous Digital Hierarchy*, синхронная цифровая иерархия, которой в Америке соответствует стандарт SONET). SDH так же, как и PDH использует временное мультиплексирование (TDM) и передают данные в цифровой форме. PDH и SDH поддерживают иерархию скоростей так, что пользователь может выбрать подходящую ему скорость для каналов, с помощью которых он будет строить вторичную (наложенную сеть). SDH и SONET совместимы и могут мультиплексировать входные потоки любого стандарта – и американского и европейского. Технология SDH обеспечивает более высокие скорости, чем PDH, так что при построении крупной первичной сети магистраль строится на технологии SDH, а сеть доступа – на технологии PDH.

9.2.3.1. Иерархия скоростей

Иерархия скоростей (уровней иерархии) SDH/SONET представлены в таблице 9.1.

Таблица 9.1. Иерархия скоростей SDH/SONET

SDH – уровни (кадры)	SONET – уровни (кадры)	Скорость
	STS-1, OC-1	51,84 Мбит/с
STM-1	STS-3, OC-3	155,520 Мбит/с
STM-3	OC-9	466,560 Мбит/с
STM-4	OC-12	622,080 Мбит/с
STM-6	OC-18	933,120 Мбит/с
STM-8	OC-24	1,244 Гбит/с
STM-12	OC-36	1,866 Гбит/с
STM-16	OC-48	2,488 Гбит/с
STM-64	OC-192	9,953 Гбит /с
STM-256	OC-768	39,81 Гбит/с

В стандарте SDH все уровни скоростей (и, соответственно, форматы этих уровней) имеют общее название *STM-N* (Synchronous Transport Module level N — синхронный транспортный модуль уровня N). В технологии SONET существует два обозначения для уровней скоростей: STS-N (Synchronous Transport Signal level N — синхронный транспортный сигнал уровня N), употребляемое в случае передачи данных электрическим сигналом, и OC-N (Optical Carrier level N — оптоволоконная линия связи уровня N), употребляемое в случае передачи данных по волоконно-оптическому кабелю. Кадры STM-N имеют достаточно сложную структуру, позволяющую агрегировать в общий магистральный порт потоки SDH и PDH порты различных скоростей, а также выполнять операции ввода-вывода без полного демультиплексирования магистрального потока. На рис. 9.3. приведена упрощенная схема мультиплексирования данных в SDH. Возможно несколько вариантов формирования SDH уровня N=1 (т.е. STM-1) из цифровых потоков E1, E3, E4 иерархии PDH. Рассмотрим процесс вложения в кадр STM-1 63 потока данных E1. На интервале 125 мкс поток данных E1 в 32 байта размещается в контейнере размером 34 байта, получившем название C-12. Увеличение размера контейнера вызвано необходимостью реализации принципа «динамического плавания» полезной нагрузки внутри контейнера. К контейнеру C-

12 добавляется один байт заголовка тракта POH (Path Overhead). В результате формируется виртуальный контейнер VC-12 (Virtual Container) размером 35 байт. В заголовке тракта VC-12 POH контейнера размещается статистическая информация о процессе прохождения контейнера вдоль пути от его начала до конечной точки: сообщения об ошибках, а также другие служебные данные, например индикатор установления соединения между конечными точками. Виртуальные контейнеры являются единицей коммутации мультиплексоров SDH. В каждом мультиплексоре существует таблица соединений (называемая также таблицей кросс-соединений), в которой указано, например, что контейнер ввода в мультиплексор VC-12 порта P1 соединен с контейнером VC-12 порта мультиплексированной магистрали P5, а контейнер VC-3 порта P8 – с контейнером VC-3 порта P9. Таблицу соединений формирует администратор сети с помощью системы управления или управляющего терминала на каждом мультиплексоре так, чтобы обеспечить сквозной путь между конечными точками сети, к которым подключено пользовательское оборудование.

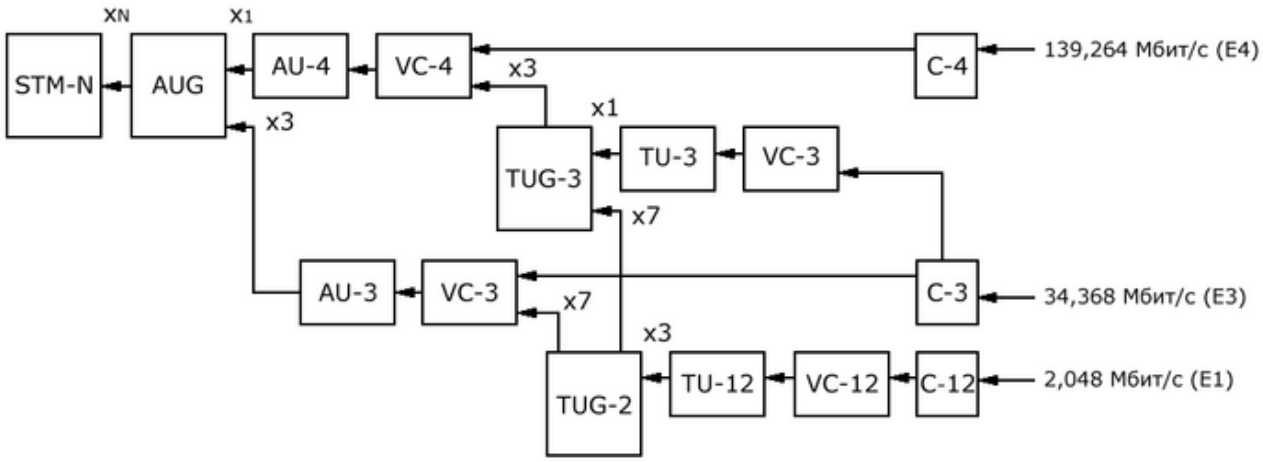


Рис. 9.3. Схема мультиплексирования потоков данных E1, E3 и E4

Для совмещения в рамках одной сети механизмов синхронной передачи кадров (STM-N) с асинхронным характером переносимых этими кадрами пользовательских данных PDH в технологии SDH применяются указатели. Концепция указателей – ключевая в технологии SDH, она заменяет принятое в PDH выравнивание скоростей асинхронных источников посредством дополнительных битов. Указатель определяет текущее положение виртуального контейнера в агрегированной структуре более высокого уровня – трибутарном блоке TU (Tributary Unit) или административном блоке AU (Administrative Unit). Собственно, основное отличие этих блоков от виртуального контейнера заключается в наличии дополнительного поля указателя. Именно благодаря системе указателей мультиплексор находит положение

пользовательских данных в синхронном потоке байтов кадров STM-N и извлекает их оттуда, чего механизм мультиплексирования, применяемый в PDH, делать не позволяет. Добавление указателя длиной в один байт к виртуальному контейнеру VC-12 превращает его в трибутарный блок TU (Tributary Unit) TU-12 длиной 36 байт. Трибутарные блоки объединены в группы, а те, в свою очередь, входят в административные блоки. Группа из N административных блоков AUG (Administrative Unit Group) и образует полезную нагрузку кадра STM-N. Помимо этого в кадре имеется заголовок с общей для всех блоков AU служебной информацией. На каждом шаге преобразования к предыдущим данным добавляется несколько служебных байтов: они помогают распознать структуру блока или группы блоков и затем определить с помощью указателей начало пользовательских данных. Три трибутарных блока TU-12 объединяются в группу TUG-2. Далее, как видно из рис. 3 формируются из каждых 7 групп TUG-2 три группы TUG-3, к каждой из которых добавляется 29 байт, состоящие из поля индикации нулевого указателя NPI (Null Pointer Indicator) и пустых байтов. Значение поля NPI равное нулю означает отсутствие контейнеров VC-3. В результате получается контейнер C-4. после добавления к нему заголовка тракта POH, состоящего из 9 байт, получаем виртуальный контейнер VC-4. Заголовок тракта в VC-4 позволяет контролировать соединение «из конца в конец». Приведем назначение некоторых байт заголовка тракта POH VC-4:

- байт, используемый в точке назначения VC-4 для подтверждения установления связи с передатчиком;
- байт проверки четности;
- байт состояния тракта, вызываемый от терминальной к исходной точке формирования тракта;
- байт, задействованный пользователем тракта для организации канала связи.

Размещение полезной нагрузки в кадре STM-1 задается указателем. VC-4 вместе с указателем называется административным модулем AU-4. На рис. 3 приведена упрощенная схема мультиплексирования по сравнения с приведенной в рекомендации ITU-T G.707 (включены только уровни иерархии европейского PDH (E1, E3, E4)). Знак xN около стрелок означает число мультиплексированных TU и TUG. Выше был приведен пример реализации кадра STM-1 из 63 потоков E1. Схема мультиплексирования SDH предоставляет разнообразные возможности по объединению пользовательских потоков PDH:

- 1 поток E3 и 42 потока E1;
- 1 поток E4

и др.

9.2.3.2. Типы оборудования SDH

Основным элементом сети SDH является мультиплексор (рис. 9.4). Обычно он оснащен некоторым количеством портов PDH и SDH: например, портами PDH E1 на 2,048 и E3 на 34,368 Мбит/с и портами SDH STM-1 на 155,520 Мбит/с и STM 4 на 622,080 Мбит/с. Порты мультиплексора SDH делятся на агрегатные и трибутарные. Трибутарные порты часто называют также портами ввода-вывода, а агрегатные - линейными портами. Эта терминология отражает типовые топологии сетей SDH, где имеется ярко выраженная магистраль в виде цепи или кольца, по которой передаются потоки данных, поступающие от пользователей сети через порты ввода-вывода (трибутарные порты), то есть втекающие в агрегированный поток («tributary» дословно означает «приток»).

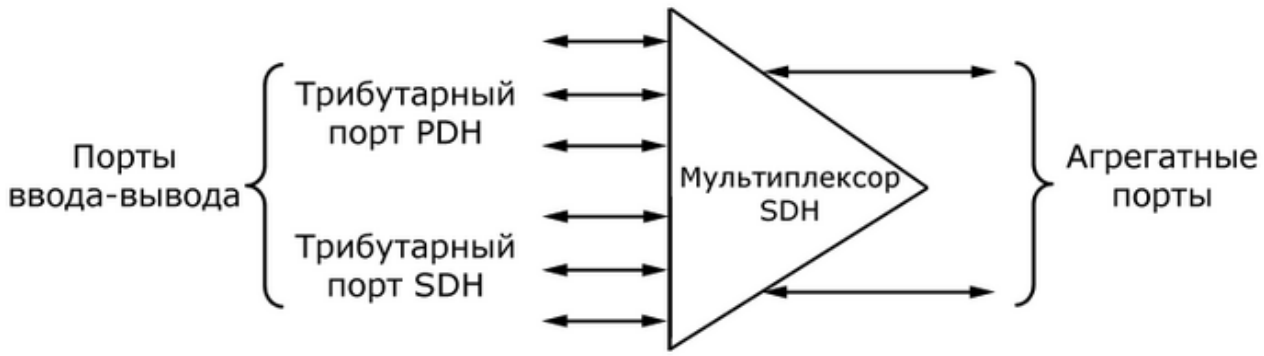


Рис. 9.4. Мультиплексор SDH

Мультиплексоры SDH обычно разделяют на два типа, разница между которыми определяется положением мультиплексора в сети SDH. Терминальный мультиплексор TM (Terminal Multiplexer) завершает агрегатные каналы, мультиплексируя в них большое количество трибутарных каналов (рис. 9.5), поэтому он оснащен не менее чем одним агрегатным портом и большим числом трибутарных портов.

Мультиплексор ввода-вывода (Add-Drop Multiplexer, ADM) занимает промежуточное положение на магистрали (в кольце, цепи или смешанной топологии). Он имеет два агрегатных порта, транзитом передавая агрегатный поток данных. С помощью небольшого количества трибутарных портов такой мультиплексор вводит в агрегатный поток или выводит из агрегатного потока данные трибутарных каналов. Помимо мультиплексоров в состав сети SDH могут входить регенераторы сигналов, необходимые для преодоления ограничений по

расстоянию между мультиплексорами. Эти ограничения зависят от мощности оптических передатчиков, чувствительности приемников и затухания волоконно-оптического кабеля. Регенератор преобразует оптический сигнал в электрический и обратно, при этом восстанавливается форма сигнала и его временные характеристики.

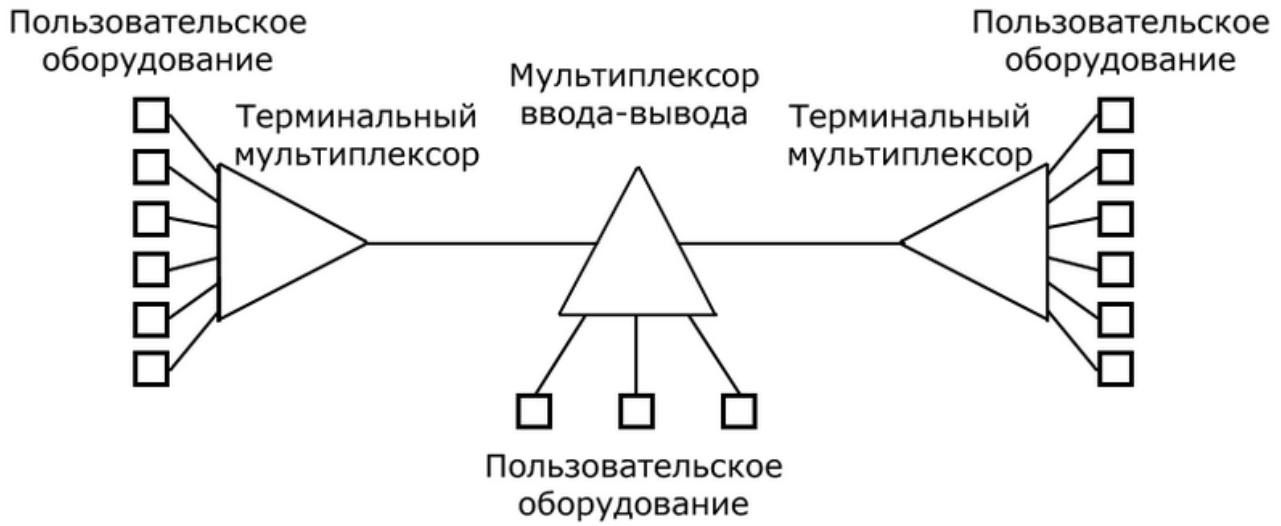


Рис. 9.5. Типы мультиплексоров SDH

9.2.3.3. Стек протоколов SDH

Стек протоколов SDH состоит из протоколов 4-х уровней. Эти уровни никак не относятся к уровням модели OSI, для которой вся сеть SDH представляет собой оборудование физического уровня.

- *Фотонный уровень* имеет дело с кодированием битов информации путем модуляции света.
- *Уровень секции* поддерживает физическую целостность сети. Регенераторной секцией в технологии SDH называется каждый непрерывный отрезок волоконно-оптического кабеля, который соединяет между собой такие, например, пары устройств SONET/SDH, как мультиплексор и регенератор, регенератор и регенератор, но не два мультиплексора. Компоненты регенераторной секции поддерживают протокол, который имеет дело с определенной частью заголовка кадра, называемой заголовком регенераторной секции RSOH (Regenerator Section

OverHead), на основе служебной информации может проводить тестирование секции и выполнять операции административного контроля.

- *Уровень линии* отвечает за передачу данных по линии между двумя мультиплексорами сети, поэтому линию также часто называют мультиплексной секцией. Протокол этого уровня работает с кадрами уровней STS-N для выполнения различных операций мультиплексирования и демультиплексирования, а также вставки и удаления пользовательских данных. Протокол линии также ответственен за реконфигурирование линии в случае отказа какого-либо ее элемента — оптического волокна, порта или соседнего мультиплексора. Служебная информация мультиплексной секции располагается в части заголовка кадра, называемой заголовком мультиплексной секции MSOH (Multiplex Section OverHead).
- *Уровень тракта* отвечает за доставку данных между двумя конечными пользователями сети. Тракт — это составное виртуальное соединение между пользователями. Протокол тракта должен принять данные, поступающие в пользовательском формате, например формате E1 и преобразовать их в синхронные кадры STM-N.

На рис. 9.6 показано распределение протоколов SDH по типам оборудования SDH.

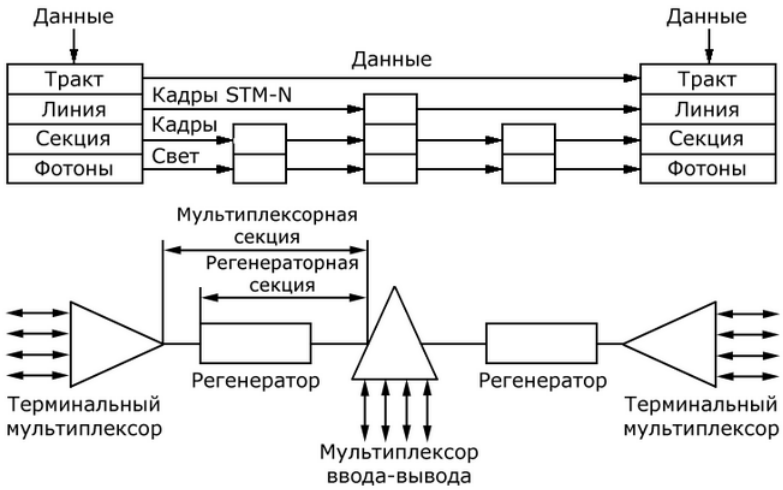


Рис. 9.6. Стек протоколов технологии SDH

9.2.3.4. Структура кадра STM

Основные элементы кадра STM-1 показаны на рис. 9.7, а в таблице 9.2 приведена структура заголовков регенераторной (RSOH) и мультиплексной (MSOH) секций. Кадр обычно представляют в виде матрицы, состоящей из 270 столбцов и 9 строк. Первые 9 байт каждой строки отводятся под служебные данные заголовков, последующие 260 байт отводятся под полезную нагрузку (данные таких структур, как AUG, AU, TUG, TU и VC), а один байт каждой строки отводится под заголовок тракта, что позволяет контролировать соединение из «конца в конец». Содержание байт заголовка тракта POH VC-4 приведено в предыдущем подразделе.

Рис. 9.7. Структура кадра STM -1

Таблица 9.2. Состав заголовка регенераторной и мультиплексной секций

Заголовок регенераторной секции RSOH	**Заголовок мультиплексной секции MSOH**
Синхробайты	Байты контроля ошибок для мультиплексной секции
Байты контроля ошибок для регенераторной секции	9 байт канала передачи данных, 576 Кбит/с
Один байт служебного аудиоканала, 64 кбит/с	Два байта, обеспечивающие переключение на резерв, индикацию аварийного состояния или отказ удаленного оборудования
Три байта канала передачи данных, 192 Кбит/с	Байт передачи сообщений статуса системы синхронизации
Байты, зарезервированные для национальных операторов связи	Остальные байты MSOH зарезервированы для национальных операторов связи

Указатель административного блока (AU-указатель) используется для указания полезной нагрузки. Полезная нагрузка может располагаться не с первой строки кадра, а после указателя и с того места (адреса), которое задаётся указателем (pointer). В действительности полезная нагрузка располагается не в одном кадре, а частично в следующем. Полезная нагрузка может смещаться в структуре кадра под действием временных флюктуаций, а указатель всегда содержит адрес начала полезной нагрузки. Для устранения последствий рассинхронизации переданного и принятого кадров STM-1 используют положительное и отрицательное выравнивание, позволяющие полезной нагрузке динамически перемещаться внутри кадра. Для этого 10-12 байты указателя можно использовать как неинформационные при положительном выравнивании. При отрицательном выравнивании 7-9 байты указателя используются как информационные. Ячейки ATM находятся в фиксированных позициях кадра. Для этого указатели в виртуальных контейнерах отмечают границы ячеек.

9.2.3.5. Топологии связей в SDH

В сетях SDH применяются различные топологии связей. Наиболее часто используются кольца и линейные цепи мультиплексоров, также находит все большее применение ячеистая топология, близкая к полносвязной (рис. 9.8).

Кольцо SDH строится из мультиплексоров ввода-вывода, имеющих, по крайней мере, по два

агрегатных порта (рис. 9.8, а). Пользовательские потоки вводятся в кольцо и выводятся из кольца через трибутарные порты, образуя двухточечные соединения (на рисунке показаны в качестве примера два таких соединения). Кольцо является классической регулярной топологией, обладающей потенциальной отказоустойчивостью — при однократном обрыве кабеля или выходе из строя мультиплексора соединение сохранится, если его направить по кольцу в противоположном направлении. Кольцо обычно строится на основе кабеля с двумя оптическими волокнами, но иногда для повышения надежности и пропускной способности применяют четыре волокна.

Цепь (рис. 9.8, б) — это линейная последовательность мультиплексоров, из которых два оконечных играют роль терминальных мультиплексоров, остальные — мультиплексоров ввода-вывода. Обычно сеть с топологией цепи применяется в тех случаях, когда узлы имеют соответствующее географическое расположение, например, вдоль магистрали железной дороги или трубопровода. Правда, в таких случаях может применяться и плоское кольцо (рис. 9.8, в), обеспечивающее более высокий уровень отказоустойчивости за счет двух дополнительных волокон в магистральном кабеле и по одному дополнительному агрегатному порту у терминальных мультиплексоров. Эти базовые топологии могут комбинироваться при построении сложной и разветвленной сети SDH, образуя участки с радиально-кольцевой топологией, соединениями «кольцо-кольцо» и т.п. Наиболее общим случаем является ячеистая топология (рис. 9.8, г), при которой мультиплексоры соединяются друг с другом большим количеством связей, за счет чего сеть может достичь очень высокой степени производительности и надежности.

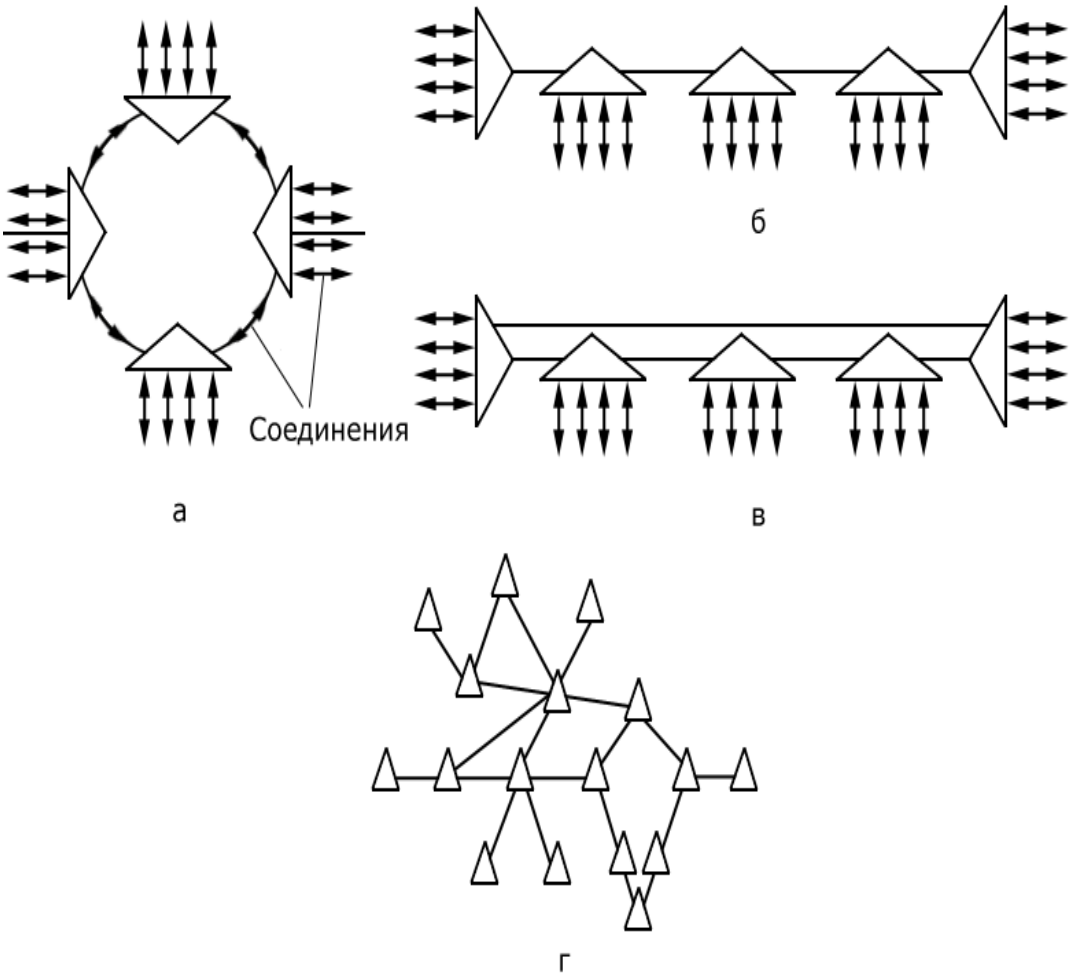


Рис. 9.8. Типовые топологии связей в SDH

ГЛАВА 10. Сеть ATM. Канальный уровень

10.1. Уровень ATM

В канальный (второй) уровень сети ATM входят уровень ATM и уровень адаптации ATM (см. рис.9.1, глава 9). На приведенном ниже рис. 10.1 показан стек протоколов уровней узлов транспортной сети и оконечных станций ATM при выполнении процедур передачи ячеек. При выполнении процедур сигнализации стек протоколов отличается и будет приведен позже в настоящей главе.

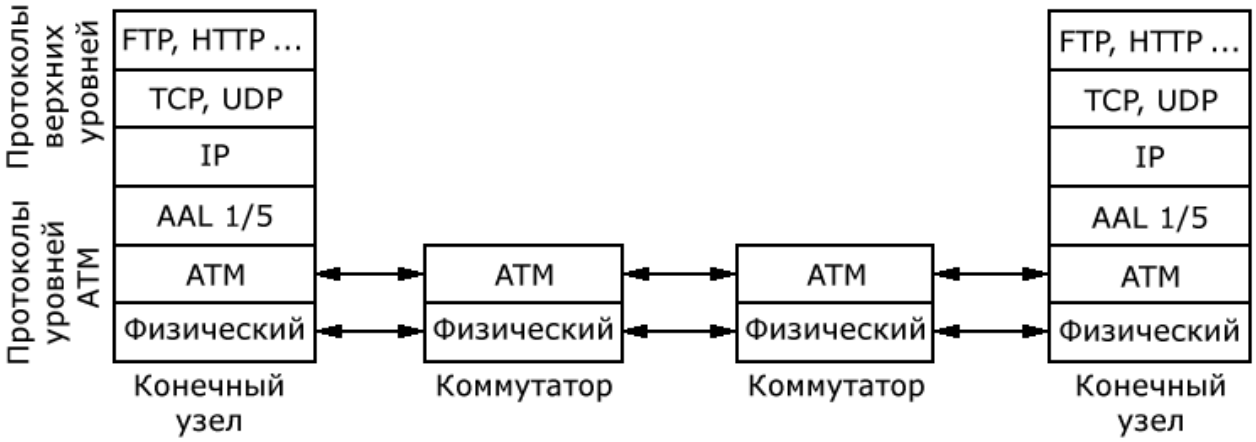


Рис. 10.1. Стек протоколов уровней ATM при выполнении процедуры передачи ячеек

Уровень ATM является частью второго уровня модели OSI. Остальная часть второго уровня относится к процедуре уровня адаптации ATM AAL, расположена в оконечной станции. Входными данными для уровня ATM на оконечной станции являются 48-байтовые элементы данных подуровня сегментации и повторной сборки SAR (Segmentation and Reassembly) уровня адаптации AAL (ATM adaptation layer). Элементы данных PDU уровня AAL пересылаются от объекта уровня в одной системе к одноранговому объекту в другой системе. Уровень ATM добавляет к этим полезным данным 5-байтовый заголовок ячейки ATM. В состав заголовка ячейки ATM входят следующие поля.

- Идентификатор виртуального пути VPI (Virtual Path Identifier) и виртуального канала VCI (Virtual Channel Identifier), служащие логическими адресами для маршрутизации ячеек.
- Тип полезной нагрузки PT (Payload Type) из трех бит:

- бит идентификатора типа нагрузки (данные пользователя или данные операций администрирования и технического обслуживания OAM - Operation, Administration and Maintenance). OAM переносит информацию управления сетью, процедуры сигнализации, маршрутизации и др.;
- бит указания того, столкнулась или нет определенная ячейка с состоянием перезагрузки в сети;
- бит, указывающий является ли ячейка последней в сообщении. В сети FR функцию сегментирования сообщений выполняют верхние уровни.

- Бит приоритета потери ячеек CLP (Cell Loss Priority) указывает на то, будет ли уничтожена ячейка в случае возникновения перегрузки. Если этот бит установлен и в сети возникла перегрузка (это состояние фиксируется в приведенном выше поле полезной нагрузки PT), то ячейка уничтожается. В противном случае она передаётся дальше. Данный бит подобен биту разрешения на уничтожение DE в сети Frame Relay (глава 8).
- Поле контроля ошибок в заголовке HEC на подуровне конвергенции физического уровня ATM при приёме ячейки либо исправляет одиночные ошибки, либо обнаруживает ошибки большей кратности и отбрасывает эти ячейки (см. главу 9).

10.1.1. Поле идентификаторов виртуального пути и виртуального канала

В отличие от технологи X.25 и FR, которые имеют одно уникальное значение для определенного интерфейса, ячейки ATM имеют два значения (на двух уровнях) – виртуальный путь VP (Virtual Path) и виртуальный канал VC (Virtual Channel). 8-разрядное для интерфейса «пользователь - сеть» и 12-разрядное для интерфейса «сеть - сеть» поле заголовка ATM используется для идентификации виртуального пути VPI (Virtual Path Identification), а 16-разрядное поле – для идентификации виртуального канала VCI (Virtual Channel Identification). Каждый из этих идентификаторов сродни уникальным значениям для определенного интерфейса LCN в X.25 и DLCI в сети FR.

В ATM могут использовать те же типы виртуальных каналов, что и в сети FR: постоянный ПВК, коммутируемый КВК и коммутируемый постоянный КПВК (т.е. соответственно PVC, SVC, SPVC). Виртуальные каналы ATM часто связывают в один виртуальный путь. Для этого служит идентификация каналов на двух уровнях – виртуальный канал VC и виртуальный путь VP. Отдельно взятый коммутатор может выполнять коммутацию канала VC, коммутацию пути VP или обе коммутации. Эти логические идентификаторы можно

рассматривать как «вложенные».

Идея комбинации значений VPI/VCI состоит в том, что идентификатор VCI рассматривается в пределах идентификатора VPI. Например, комбинация 3/40 обозначает, что используется значение идентификатора виртуального канала (VCI), равное 40, для идентификатора виртуального пути VPI, равного 3. Комбинация двух идентификаторов является идентификатором соединения. Виртуальный путь VP содержит множество виртуальных каналов (Virtual Circuits – VCs), а виртуальное канальное соединение (Virtual Circuit Connection – VCC) содержит множество путей VP.

Связывание виртуальных каналов обычно формирует один VP, а связанные VP, как правило, находятся в одном физическом канале передачи. Следует отметить, что 24 бита, выделенные для полей VPI/VCI в заголовке ячейки ATM, могут поддерживать максимум 16888216 пользователей в одном физическом канале ATM! Учитывая высокие скорости передачи данных на физическом уровне ATM до нескольких терабит в секунду (при использовании технологии волнового мультиплексирования), не представляется невероятным то, что миллионы пользователей смогут совместно использовать один канал передачи данных. Так же следует заметить, что определенные значения VPI/VCI зарезервированы для использования в сетевом управлении и задач управления ресурсами, таких как сообщения и отчеты о неисправности сети. Для иллюстрации коммутации в сети ATM приведем пример иерархической адресации VPI/VCI при использовании постоянных виртуальных каналов PVC .

Предположим, что необходимо создать схему адресации ATM-сети на основе PVC-каналов с учетом того, что она состоит из трех филиалов, которые в трех крупных штатах США: Калифорния, Техас и штат Нью-Йорк (рис. 10.2). В каждом из штатов необходимо соединить ATM-каналами по три крупных города. В штате Калифорния – Сан-Франциско, Лос-Анджелес и Сан-Хосе. В штате Техас – Хьюстон, Даллас и Ости; в штате Нью-Йорк – Буффало, Нью-Йорк и Олбани. В результате анализа трафика был сделан вывод, что наиболее эффективной в создаваемой структуре будет полносвязная топология. Поэтому чтобы упростить управление сетью, было принято решение о создании иерархической схемы адресации, в которой каждому из трех штатов будет соответствовать только один идентификатор – номер VPI. Чтобы установить соединение с коммутатором в некотором из штатов, необходимо указать город, добавив другой уникальный адресный идентификатор – VCI. Рассмотрим данный процесс на конкретном примере, когда коммутатор, анализируя ячейки, которые поступают из базовой сети, определяет, что в них установлено значение VPI

равное 9. Это означает, что данный трафик необходимо направить к коммутатору штата Калифорния. Если значение равно 11, то трафик должен быть перенаправлен в Нью-Йорк, если 5 – в Техас. Далее выполняется второй уровень коммутации, когда для определения города, в который необходимо направить данные, анализируются оба значения: и VPI и VCI. Например, коммутатор штата Калифорния переправляет ячейки, значение VPI которых равно 9, а значении VCI равно 181 в Сан-Франциско. Соединяться с любым штатом можно зная только значение VPI. Следует заметить, что значение VPI, так же как и значения VCI, имеют только локальное значение для каждого интерфейса коммутатора. Когда рассматривают виртуальное соединение, то подразумевают, что коммутатор АТМ переправляет ячейки, основываясь на полной комбинации значения VPI/VCI.

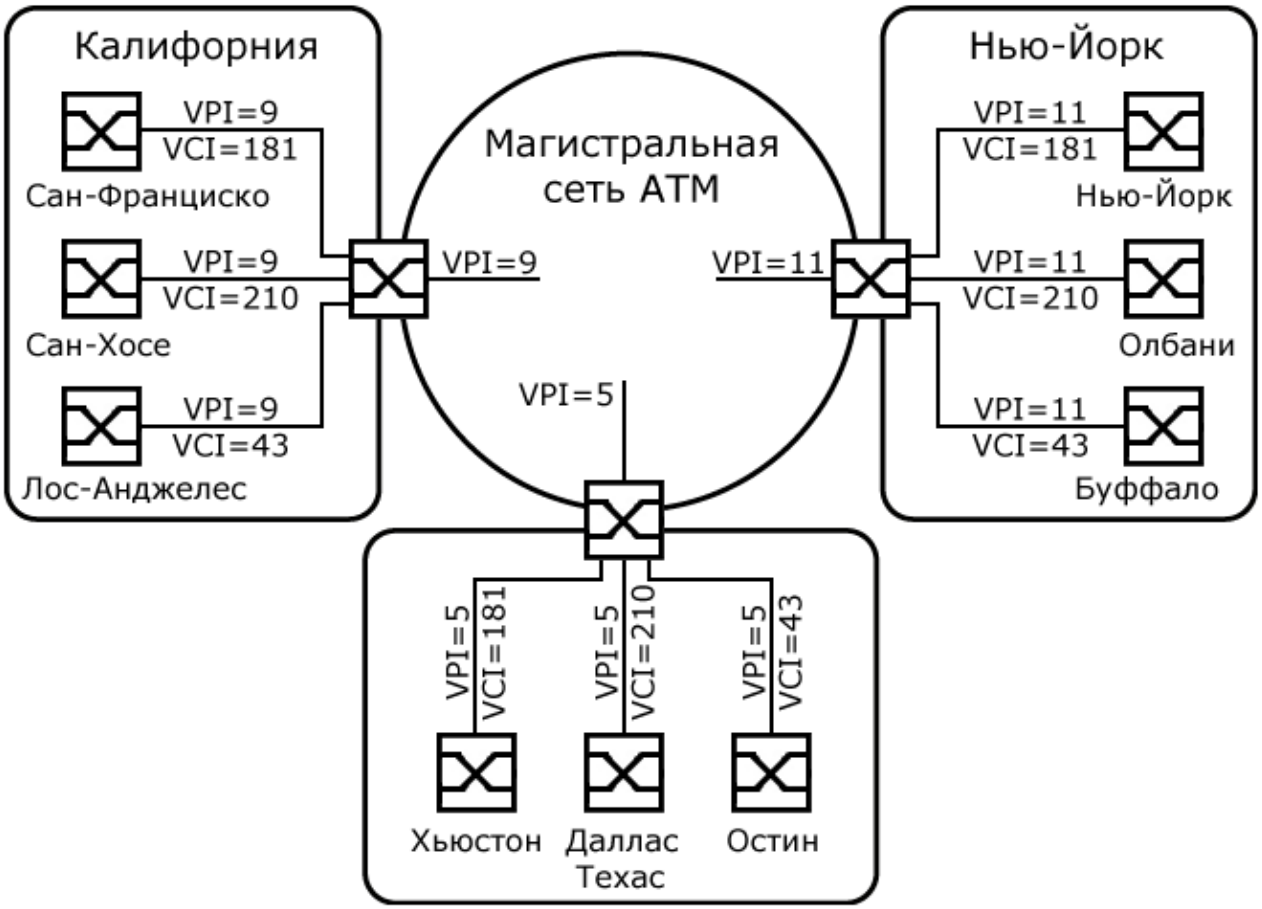


Рис. 10.2. Пример иерархической адресации VPI/VCI в сети АТМ

10.2. Параметры трафика и показатели качества обслуживания

Для сети ATM определено четыре класса служб (табл. 10.1), охватывающих весь спектр мультимедийного характера трафика.

Таблица 10.1. Классы служб ATM

Класс служб	A	B	C	D
Режим соединения	С установлением соединения			Без установления соединения
Скорость	Постоянная	Переменная		
Тип трафика	Постоянная скорость для передачи речи, аудио, видео	Сжатые речь, аудио, видео	Передача данных для банковских транзакций и др.	Передача данных без установления

Служба класса A предназначена для поддержки аудио и видео-приложений, где информацию нужно передавать с постоянной скоростью. *Службы класса B* обеспечивает передачу уплотненного речевого, аудио или видео-трафика, поэтому трафик носит пульсирующий характер, а скорость пересылки данных может изменяться. *Служба класса C* обеспечивает передачу данных пакетной коммутацией. *Служба класса D* предназначена для передачи данных без установления соединения. Каждый пакет, передаваемый в сеть, содержит полные адреса отправителя и получателя. Не гарантируется потеря ячеек. Такая доставка по возможности («best effort») либо не ставит задачу надежного обмена с гарантией показателя вероятности потери ячеек, либо предусматривается восстановление потерянных ячеек на верхнем уровне, т.е. в оконечной станции.

В сети пакетной коммутации Frame Relay для установления виртуального соединения предусмотрен только один параметр трафика — согласованная скорость передачи CIR, которую сеть обязана поддержать при обычных условиях (глава 8). В мультимедийной сети ATM для установления виртуального соединения по запросу пользователя предусмотрены следующие параметры трафика:

- *PCR (Peak Cell Rate)* – верхняя граница скорости передачи ячеек, указывающая на

максимальное количество ячеек, переданных за одну секунду.

- *SCR (Sustained Cell Rate)* – средняя скорость передачи ячеек, указывающая на согласованный верхний уровень среднего количества ячеек, которое может быть передано за одну секунду.
- *MCR (Minimum Cell Rate)* – минимальная скорость передачи ячеек, с которой отправитель может передавать данные.
- *MBS (Maximum Burst Size)* – максимальная величина пульсации, указывающая на максимальное количество ячеек для скорости PCR, которые могут быть переданы по некоторому соединению.
- *CDVT (Cell Delay Variation Tolerance)* – максимально допустимое отклонение задержки ячеек. В отличие от Frame Relay в сети ATM при установлении виртуального соединения пользователю предоставлена возможность затребовать гарантию обеспечения следующих характеристик качества обслуживания QoS.
- *MCTD (Maximum Cell Transfer Delay)* – максимальная задержка при передаче ячеек, определяемая временем задержки при передаче ячеек, определяемая временем передачи ячейки от одной оконечной станции к другой.
- *CDV (Cell Delay Variation)* – амплитуда отклонения задержки ячеек. Изменения времени между двумя последовательными передачами называется флюктуацией фазы или джиттером. Это вызывает искажения видео или речи, которые выражаются в дрожании. Согласно спецификации ATM-форума значение CDVT является параметром трафика, а не параметром QoS и поэтому не требует уникальной величины при установлении соединения. На рис. 10.3 приведены примеры сильной и слабой флюктуации.

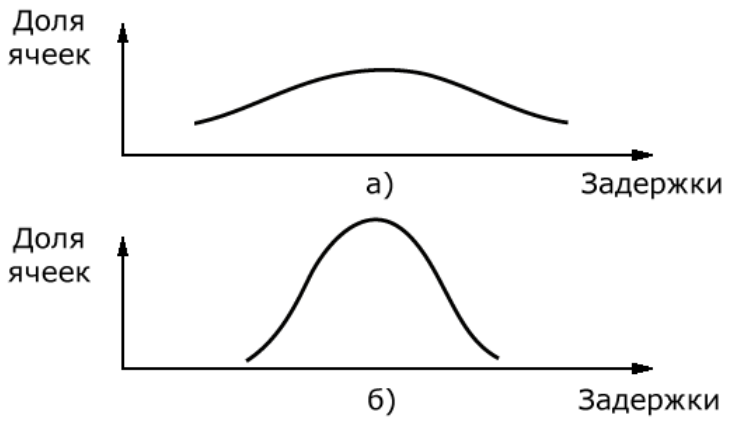


Рис. 10.3. Примеры сильной (а) и слабой (б) флюктуации

- *CLR (Cell Loss Ratio)* – вероятность потери ячеек, равная отношению потерянных к общему числу переданных ячеек.

Установление коммутируемого виртуального канала в сети ATM во многом похоже на то, как это осуществляется в сети Frame Relay на приведенной на диаграмме рис. 5 (глава 8). В следующих разделах будет отмечены отличия в сети ATM, вызванные в первую очередь мультимедийными возможностями сети.

10.3. Уровень адаптации ATM

Для поддержки классов трафика и обеспечения пользователю гарантий качества обслуживания на оконечных пунктах сетей ATM предусмотрены протоколы адаптации AAL (ATM Adaptation Layer). Форумом ATM стандартизировано четыре типа протоколов AAL: AAL1, AAL2, AAL¾, AAL5Эти протоколы соответствуют части второго уровня эталонной модели OSI (см. рис. 10.1). В зависимости от конкретного вида информации пользователя (речь, видео или данные) и класса служб (A,B,C или D) используется определенный тип протокола AAL. В таблице 10.2 приведены сервисы AAL и соответствующие им классы трафика, гарантированные пользователю показатели качества обслуживания (QoS) и используемые для реализации типы протоколов AAL. Сервису с постоянной битовой скоростью CBR (Constant Bit Rate) соответствует тип трафика класса службы A. Согласованию пользователя с сетью подлежат параметры трафика PCR и CDVT, показатели задержки и потерь ячеек. Для реализации используется протокол AAL1. Типичные применения CBR включают телефонию, телевидение, радио, видео по требованию. Сервису с переменной битовой скоростью реального времени rt-VBR (real-time Variable Bit Rate) соответствует тип трафика класса службы B. Согласованию пользователя с сетью подлежат

параметры трафика PCR, CDVT, SCR, MBS, показатели задержки и потерь ячеек. Для реализации используется протокол AAL2. Типичные применения rt-VBR сжатая речь, аудио и видео. Сервису с переменной битовой скоростью нереального времени nrt-VBR (non-real-time Variable Bit Rate) соответствует тип трафика класса службы С. Согласованию пользователя с сетью подлежат параметры трафика PCR, CDVT, SCR, MBS, показатель потерь ячеек. Для реализации используется протокол адаптации AAL5. Поскольку класс трафика С относится к службе передачи данных, то используемый протокол AAL5 не гарантирует показатель задержки ячеек.

Таблица 10.2. Сервисы AAL, классы и параметры трафика, гарантированные QoS и типы AAL

Сервисы AAL	Классы службы	Параметры трафика	Гарантированные QoS		Типы AAL
			Задержки ячеек	Потери ячеек	
CBR	Класс А	PCR, CDVT	да	да	AAL1
rt-VBR	Класс В	PCR,SCR,MBS,CDVT	да	да	AAL2
nrt-VBR	Класс С	PCR,SCR,MBS,CDVT	нет	да	AAL5
UBR	Класс С	PCR, CDVT*	нет	нет	AAL5
	Класс D	PCR, CDVT*			AAL¾
ABR	Класс С	PCR, MCR,CDVT	нет	да	AAL5
	Класс D	PCR, MCR,CDVT			AAL¾

* необязательный для соблюдения параметр

Сервис неопределённой битовой скорости UBR (Unspecified Bit Rate) соответствует трафику классов С и D. С пользователем в этом случае согласуется только параметр PCR. UBR не гарантирует никакой параметр QoS. Реализуется UBR с помощью протоколов AAL¾ или AAL5. Чем меньше загружена сеть, тем больше вероятность доставки ячеек. Несмотря на высокую вероятность потери ячеек UBR применяется для некритичных приложений: проверка кредитных карт (если попытка не удалась, то пользователь попробует еще раз), электронная почта, факсимильные сообщения и др. Сервис доступной битовой скорости ABR (Available Bat Rate) соответствует трафику классов С и D. При этом с пользователем согласуются параметры PCR и MCR. Пользователь начинает передачу на скорости MCR и далее увеличивает скорость, пока сеть не укажет на высокую вероятность потерь ячеек. Тогда скорость снижается до малой вероятности потерь. Для ABR сеть гарантирует вероятность доставки ячеек, отправленных со скоростью равной или меньшей MCR. Сервис ABR

позволяет оконечным станциям адаптировать их трафик к текущему состоянию сети. Это осуществляется с помощью сообщений обмена сети с пользователем по специальному виртуальному каналу. Отметим, что параметр трафика во многом похож на согласованную скорость передачи CIR в сети Frame Relay (глава 8). Как видно из рис. 10.4 уровень адаптации AAL делится на два подуровня. Нижний подуровень AAL является подуровнем сегментации и повторной сборки (восстановления) SAR (Segmantation and Reassembly), а верхний подуровень AAL – подуровень конвергенции CS (Convergence Sublayer). Основная функция AAL заключается в объединении (адаптации) разных трафиков и разных сервисов в инфраструктуре ATM. На рис. 10.4 приведена общая схема операций стека протокола сети ATM. Подуровень CS необходим для конкретного типа предоставления служб и включает подуровень специфический для служб (SSCS) и общий (CPCS). Подуровень SSCS зависит от приложений и в некоторых случаях может отсутствовать. Подуровень CPCS необходим всем пользователям конкретного типа службы.

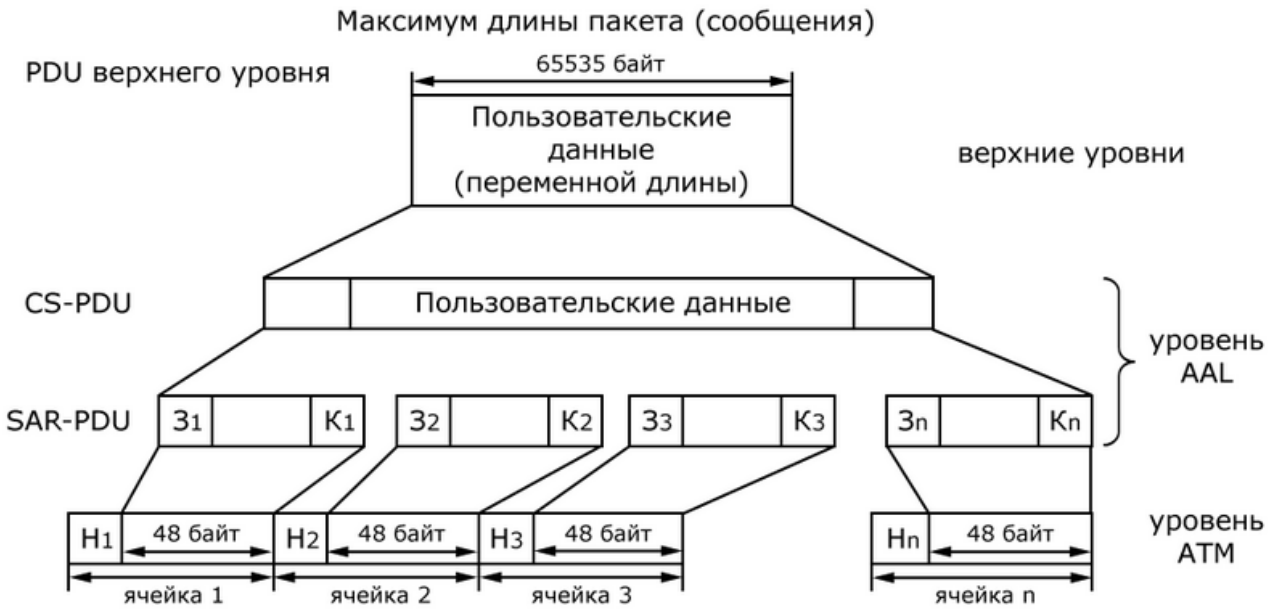


Рис. 10.4. Операции протоколов сети ATM

На рис. 10.4 приняты следующие обозначения:

- З, К – соответственно заголовок и концевик блока сообщения подуровня CS;
- $З_1$ $К_1$, $З_1$ $К_2$, $З_3$ $К_3$... $З_n$ $К_n$ – соответственно заголовки и концевики сегментов подуровня SAR;
- $Н_1$,$Н_2$, $Н_3$ …$Н_n$ – заголовки ячеек уровня ATM. Рассмотрим операции стека сверху вниз.

Рассмотрим операции стека сверху вниз. Элемент данных протокола PDU (пакет, сообщение) верхнего уровня поступает на вершину стека протоколов ATM на оконечной станции и попадает на подуровень конвергенции CS. В результате добавления служебной информации в виде заголовка (З) и концевика (К) формируется CS-PDU. Каждый тип AAL включает разное содержание в служебную информацию. CS-PDU, переданный на подуровень SAR, сегментируется на блоки длиной 48 байт SAR-PDU), включая в них специфическое содержание для каждого типа AAL в служебную информацию заголовков и концевиков ($З_1$ $К_1$; $З_2$ $К_2$; $З_3$ $К_3$... $З_n$ $К_n$). Эти модули передают на уровень ATM, где к ним добавляются 5 байт заголовка ($Н_1$,$Н_2$, $Н_3$ …$Н_n$) формирующие ячейки. Затем ячейки поступают на физический уровень ATM. На принимающей стороне процесс, показанный на рис. 10.4, происходит в обратном порядке. Результатом является возможность интегрировать множество типов трафика в одну коммутируемую структуру. В SAR-PDU служебная информация, относящаяся к типу AAL1 и гарантирующая только задержку, содержится только в заголовке и включает последовательный номер ячейки (для проверки на потерянные, неверно выставленные или испорченные ячейки). В модуле SAR-PDU служебная информация, относящаяся к типу AAL¾, содержится в заголовке и кон цевике. Концевик здесь включает контрольно-проверочную комбинацию циклического кода для обнаружения и коррекции ошибок в пользовательских данных. Длина этой комбинации составляет 10 бит для проверки 44 байт полезной информации. Протокол AAL5 используется также как и AAL¾ для предоставления классов служб C, D и определён в качестве альтернативы из-за его сложности. Подуровень конвергенции CPCS AAL5 включает концевик, содержащий 4 байта контрольно-проверочной комбинации циклического кода для обнаружения ошибок в элементе данных и 2 байта для указания длины пользовательских данных.

Протоколы AAL3/4, ALL5 относится к службе передачи данных и производят повторную передачу испорченных элементов CS-PDU, обеспечивая при этом высокий показатель QoS по вероятности потерь.

10.4. Сигнализация и маршрутизация в сети ATM

Процесс сигнализации в сети ATM (установление, поддержка и разъединение коммутируемых виртуальных каналов) во многом похож на эту процедуру в сети Frame Relay (диаграмма, которой приведена на рис. 8.5, глава 8). Приведем основные отличия в сети ATM.

1) В коммутаторах и оконечных станциях сети ATM используется протокол Q.2931, который в отличие от Q.931 (используемого в сети FR) кроме двухуровневого идентификатора виртуального канала в состав сообщения запроса на установку соединения SETUP дополнительно включает:
   - показатели качества обслуживания QoS, к которым могут относится все приведенные в разделе 10.2 (максимальная задержка при передаче ячеек MCTD, амплитуда отклонения задержки CDV, вероятность потерь ячейки CLR) или некоторые из них;
   - показатели трафика в зависимости от классов трафика, к которым могут относиться приведенные в разделе 10.2 и таблице 10.2;
   - уровень адаптации AAL.
2) стандартизации подлежат процедуры протокола не только «пользователь-сеть» (которым соответствует диаграмма установления коммутируемого виртуального соединения в сети FR на рис 8.5, глава 8), но и процедуры протокола между ATM-коммутаторами.

Интерфейс подключения конечных пользователей к ATM-коммутатору обозначается UNI (User-Network Interface). Интерфейс между ATM-коммутаторами обозначается NNI (Network Node Interface).

10.4.1. Стек протоколов при установлении коммутируемого виртуального канала

На рис 10.5 приведена упрощенная схема стека протоколов сигнализации установления коммутируемого виртуального канала. Для обслуживания требуемого уровня обслуживания QoS оконечные станции и сеть должны выделить для виртуального соединения достаточное количество ресурсов.

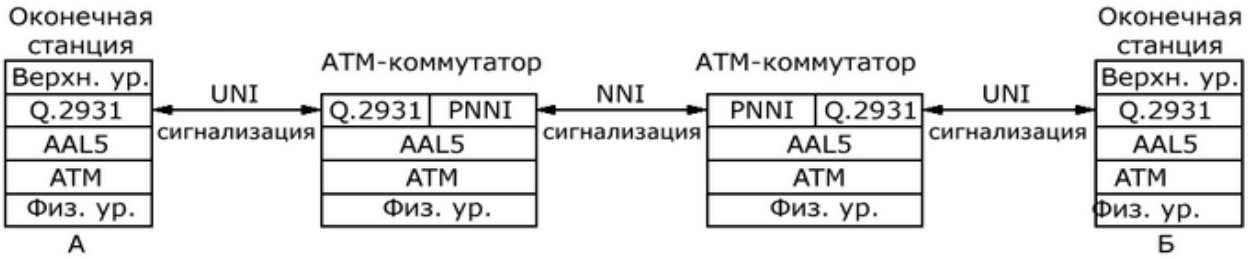


Рис. 10.5. Стек протоколов сигнализации при установлении коммутируемого виртуального канала

Рассмотрим установление коммутируемого виртуального канала в самом общем виде. Предположим, что необходимо установить соединение между оконечными станциями А и Б. Оконечная станция А, используя протокол Q.2931, отправляет на граничный АТМ-коммутатор служебное сообщение SETUP запроса на установление коммутируемого виртуального канала (КВК). Как было отмечено выше, это сообщение включает физические адреса А и Б (например, по стандарту Е.164), требования пользователя к сети о предоставлении параметров трафика и качества обслуживания. Это сообщение предаётся протоколу, использующему уровень адаптации AAL5. 48-байтовые блоки сегментации и повторной сборки SAR (рис. 10.4) передаются на АТМ уровень, на котором к ячейкам протокола Q.2931 добавляется заголовок с VPI равным X и VCI-значением равным 5. Когда ячейки поступают в первый коммутатор (по протоколу UNI), он знает, что это ячейки сигнализации. Этот коммутатор удаляет заголовки ячеек, осуществляет повторную сборку 48-байтовых блоков полезной нагрузки и проверку ошибок на уровне AAL5. После того, как отправлено сообщение SETUP на интерфейсе UNI от оконечной станции необходимо удостовериться, что при заданных пользователем показателях трафика могут быть предоставлены ему заданные в сообщении показатели QoS. При этом не должны быть нарушены условия, при которых ранее были установлены соединения. Для этого применяется специальный алгоритм управления доступом к соединениям CAC (Connection Admission Control). Алгоритм CAC определяет можно ли принять или следует отклонить запрос на соединение. Входной коммутатор запускает алгоритм CAC и определяет при положительном решении, что его ресурсы отвечают выдвигаемым требованиям QoS. Теперь стоит задача кто будет следующим транзитным коммутатором, который сможет соответствовать заданному требованию QoS?

Эту функцию выполняет стандартизированный форумом АТМ протокол PNNI (Private Network-to-Network Interface), который включает процедуру маршрутизации и процедуру сигнализации.

10.4.2. Протокол PNNI по выполнению функции маршрутизации

Протокол PNNI по выполнению функции маршрутизации отвечает за распространение между коммутаторами ATM и группами коммутаторов ATM информации об изменении топологии сети. Протокол PNNI по выполнению функции сигнализации основан на дополнительных возможностях процедуры сигнализации на интерфейсе UNI, которые заключаются в использовании возвратных маршрутов. *PNNI* – это протокол маршрутизации с учётом состояния каналов. Он позволяет использовать разделённые области за счёт иерархической структуры сети, поддерживает маршрутизацию с учётом уровня качества обслуживания QoS и др. Иерархическая структура позволяет скрыть сетевые изменения в одной области от другой, что приводит к изолированию областей сети, несмотря на то, что в основу положен метод информирования о состоянии канала. Единственным недостатком такой инфраструктуры является возможная маршрутизация в неопределенную область. Протокол PNNI позволяет определить наиболее подходящий маршрут для запрашиваемого QoS. В информационных элементах сигнального сообщения отправителя содержится полный путь, предоставленный входным коммутатором (рис. 10.6). Такой механизм называется маршрутизацией от источника. Определение «наилучшего маршрута» в протоколе происходит совсем по-другому, нежели в других протоколах, таких как OSPF IP-сети. Протокол OSPF определяет наилучший по стоимости маршрут, а протокол PNNI определяет наилучший маршрут, который соответствует требуемому уровню QoS для определённого соединения.

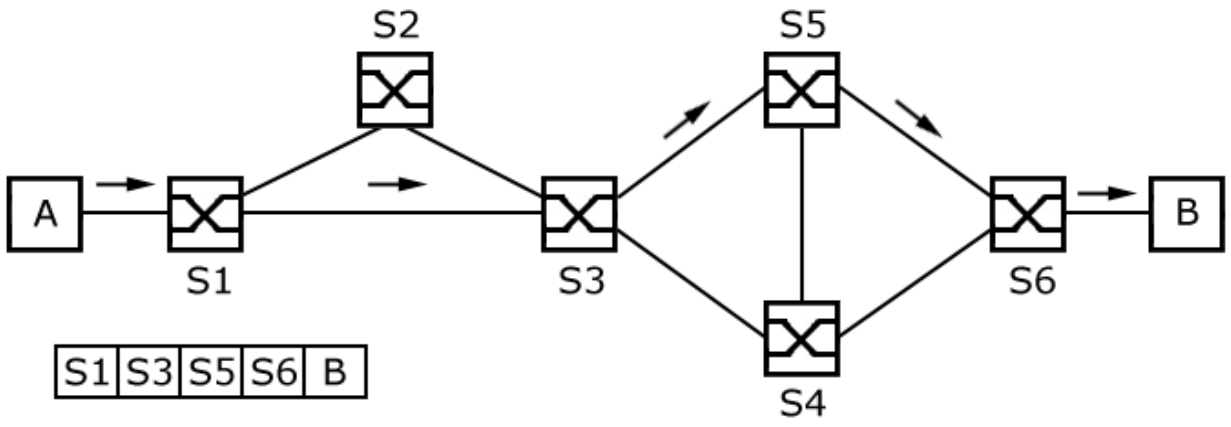


Рис. 10.6. Механизм маршрутизации от источника

При использовании иерархической структуры маршрутизаторы разбиваются на отдельные области (как и в ТфОП отдельные местные сети, зоновые сети). Каждый маршрутизатор знает все детали выбора маршрута в пределах своей области, но ему ничего неизвестно о внутреннем строении других областей. Если иерархия не используется, то каждому маршрутизатору в этой плоской структуре необходимо поддерживать таблицу маршрутизации из всех N строк (по числу маршрутизаторов в сети). Если сеть разбить на Z областей с числом маршрутизаторов в каждой области N/Z, то каждому маршрутизатору потребуются значительно меньшая таблица маршрутизации, равная N/Z локальных записей в каждой области плюс Z-1 записей об удаленных областях. Допустим N = 720. При Z=1 (одноуровневая структура) число записей равно 720, а при Z=24 число записей равно 53. Иерархическая структура для больших сетей позволяет сократить объём памяти для хранения таблиц маршрутизации и времени обработки таблицы центральным процессором. Процедура протокола PNNI анализирует каждый запрос на соединение индивидуально на основании показателей QoS в сообщении SETUP. Если где-либо в сети произошло изменение уровня обслуживания QoS, то происходит лавинная рассылка элементов состояния PNNI-топологии PTSE (PNNI Topology State Element), в результате чего производится изменение маршрутизации внутри группы узлов сети. Элементы PTSE состояния PNNI-маршрутизации распространяются с помощью специальных пакетов PTSP (PNNI Topology State Packet). Пакеты PNNI-маршрутизации распространяются по специальному выделенному виртуальному каналу с идентификаторами VPI = 0, VCI = 18.

10.4.3. Протокол по выполнению функции сигнализации PNNI

Протокол PNNI по выполнению функции сигнализации завершает доставку сигнального сообщения SETUP, запрашиваемого пользователем на установление соединения со стороны интерфейса UNI. Протокол PNNI по выполнению функции сигнализации использует:

- маршрут от источника, определённый протоколом PNNI по выполнению функции маршрутизации;
- информацию о достижимости, возможности установления соединения из результатов работы протокола PNNI по выполнению функции маршрутизации;
- механизм обратного маршрута, который допускает временное разъединение незавершённого соединения из-за несоответствия уровня обслуживания QoS или повреждения канала связи.

На рис. 10.6 приведён пример сигнализации PNNI в плоской иерархической сетевой топологии. С оконечного устройства A на интерфейс UNI приходит сигнальный запрос SETUP. Полученный данный запрос на коммутаторе S1 с помощью алгоритма CAC определяет можно ли принять или следует отклонить запрос. С помощью QoS в сообщении SETUP и метрик QoS в списке узлов одной PNNI-группы равноправных узлов (в данном случае узлов S2,S3,S4,S5,S6), узел S1 может составить список транзитной передачи этой группы узлов DTL (Designated Transit List). DTL полностью определяет маршрут через одну PNNI-группу равноправных узлов. SETUP передаётся следующему в списке DTL коммутатору S3, который также запускает алгоритм CAC. Коммутатор S3 в случае соответствия требованиям оконечного пункта A вычисляет ожидаемое поведение других узлов. Теперь SETUP передаётся к следующему в списке DTL коммутатору S5, который выполняет те же операции, что и S3. Допустим, что он также соответствует требованиям оконечного пункта A. Теперь SETUP передаётся к S6. Наконец, коммутатор S6 передаёт SETUP оконечного пункта A получателю (оконечному пункту B), который генерирует ответ «CONNECT». Теперь представим другую ситуацию, когда в сети вместо шести узлов, как показано на рис. 10.6, находится 100. Пусть топология в данном случае тоже будет плоской. Допустим, что в процессе передачи SETUP один из коммутаторов, например, с номером 50, отклоняет запрос на соединение, т.е. не выполняет требования пользователя по QoS и трафику. Следовательно, механизм обратного маршрута необходимо применить к точке входа в ATM-сеть, т.е. к коммутатору S1. При этом появляется большой дополнительный трафик и увеличивается время установления соединения. Для разрешения такой ситуации в широкомасштабных сетях используется иерархическая топология сети. При этом не требуется возврат в исходную точку в сеть в том случае, когда коммутатор в списке DTL не отвечает QoS требованиям в сообщении SETUP. Коммутатору, определившему список DTL, отправляется сообщение разрыв соединения (RELEASE). Получив это сообщение этот коммутатор, принадлежавший той же группе, пытается найти альтернативный маршрут, который отвечал бы требованиям QoS.

10.5. Управление ATM-трафиком в процессе передачи

После того, как было установлено соединение согласно требуемому пользователем уровню качества обслуживания QoS и соблюдены условия соглашения о трафике, сеть готова к передаче ячеек. Соглашение о трафике является чем-то вроде «закона» в данном соединении. Допустим, что некоторая станция нарушает и передаёт значительно больше трафика, чем оговорено в соглашении. Существуют две основные функции управления трафиком: *контроль трафика* и *контроль перегрузок*.

10.5.1. Контроль трафика

Основной функцией контроля трафика является мониторинг соединения. При этом производится мониторинг потока трафика и соблюдения условий соглашений в целях защиты сетевых ресурсов от неправильного использования (или злоупотребления), которое может преднамеренно или непреднамеренно повлиять на качество услуг, предоставляемых другим пользователям сети по установленным ими соединениям. Мониторинг соединений на NNI-уровне является обязательным и называется NPC (Network Parameter Control). Приведём один из самых простых механизмов мониторинга и контроля трафика с NNI-интерфейса. В случае нарушения ячейкой соглашения о трафике, входной коммутатор устанавливает бит приоритета потери CLP (Cell Loss Priority), равным 1, тем самым отмечая, что у неё низкий приоритет. Если же ячейка не нарушила условия соглашения пользователя с сетью, её бит CLP остаётся равным 0, что указывает на высокий приоритет. При возникновении перегрузки в сети ячейки с приоритетом 1 уничтожаются, а с приоритетом 0 передаются дальше. Форум ATM определяет две модели проверки приоритета.

- Модель прозрачной передачи битов CLP, при которой устройство сети игнорирует CLP-бит. Такая модель используется, например, при сервисе AAL с постоянной битовой скоростью CBR, для которого важна гарантия показателя задержки ячеек.
- Модель пристальной проверки CLP, при которой применяется селективное уничтожение ячейки с CLP-бит, равным 1. Такая модель используется, например, в сервисе AAL net-VBR, для которого важна гарантия показателя вероятности доставки пакета.

10.5.2. Контроль перегрузки

Форум ATM специфицировал два метода контроля перегрузки.

- Индикация явной перегрузки при прямой передаче EFCI (Explicit Forward Congestion Indication).
- Относительная маркировка скорости передачи RRM (Relative Rate Marking).

В режиме EFCI коммутатор устанавливает в заголовке ячейки соответствующий бит. Приняв такую ячейку, оконечная станция-получатель адаптивно понижает скорость ячеек в соединении. Если в таких соединениях используются ячейки управления ресурсами RM-ячейки с определенными значением VCI=6, оконечная станция-получатель может уведомить отправителя о перегрузе. Для этого станция-получатель посылает RM-ячейку с указанием о

перегрузе на оконечную станцию отправителя. Сервисы AAL CBR, nrt-VBR, rt-VBR, UBR могут использовать режим EFCI. В режиме RRM оконечная станция-отправитель периодически генерирует и посылает во все соединения вместе с ячейкам данных RM-ячейки. Устройство-получатель отправляет их назад отправителю, определяя тем самым, испытывает ли промежуточный коммутатор перегрузку. В RRM режиме коммутатор сам может уведомлять о перегрузке, а в EFCI получатель уведомляет отправителя о перегрузке. Поэтому режим RRM более эффективен. Метод RRM является обязательным для сервиса ABR.

10.6. Виртуальная частная сеть на основе сети ATM

Для построения VPN используются постоянные виртуальные каналы, в которых значения

VPI/VCI устанавливаются администратором сети. На рис. 10.7 приведена логическая структура VPN-сетей ATM.

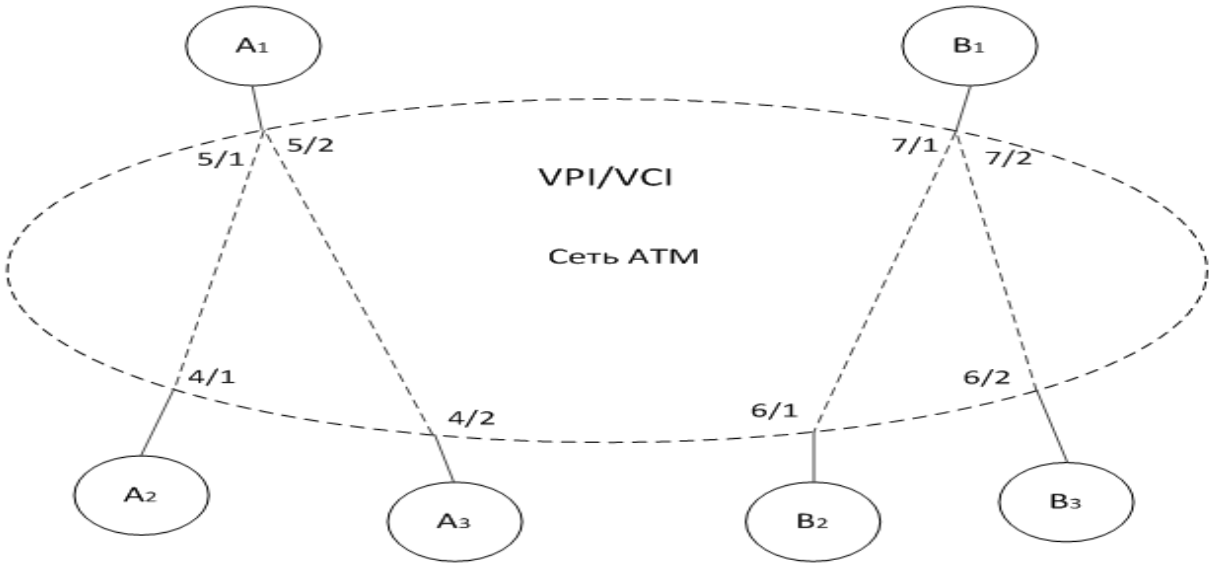


Рис. 10.7. Логическая структура VPN-сетей ATM

На этом рисунке показаны виртуальные соединения двух VPN-сетей ATM – пользователей офисов компании A и компании B. На рисунке не показаны коммутаторы ATM. VPN-сети на основе ATM отличаются от VPN-сетей FR тем, что виртуальные каналы предоставляются широким набором согласованных показателей качества обслуживания QoS. Первая VPN A пользователей центрального офиса A1 и двух его филиалов – A2 и A3. ATM предоставляет виртуальные каналы между главным офисом и филиалами с номерами идентификаторов VPI/VCI =5/1 и 5/2, 4/1, 4/2 (созданных в оконечных коммутаторах ATM с соответствующими офисами A1, A2, A3). Аналогично вторая VPN B включает пользователей

центрального офиса В1 и двух его филиалов – В2 и В3. АТМ предоставляет виртуальные каналы между главным офисом и филиалами с номерами идентификаторов VPI/VCI =7/1 и 7/2, 6/1, 6/2 (созданных в оконечных коммутаторах АТМ с соответствующими офисами В1, В2 , В3). Пользователи каждой VPN получают по виртуальным каналам доступ только к пользователям своей VPN.

10.7. Особенности сети АТМ по сравнению с сетью Frame Relay

- АТМ – мультимедийная сеть, предназначенная для передачи любого вида служб. Frame Relay в соответствии со спецификацией является сетью только передачи данных.
- АТМ обеспечивает передачу данных в двух режимах – с установлением и без установления соединения. Frame Relay обеспечивает работу только в режиме с установлением соединения.
- Стек протоколов оконечных станций АТМ включает уровни адаптации AAL предоставляющие различные процедуры обработки данных в зависимости от вида службы (речь и видео, сжатое видео и речь, передача данных с установлением или без установления соединения). В сети Frame Relay отсутствуют уровни адаптации.
- Для выполнения функций сигнализации в стек протоколов оконечных станций и коммутаторов АТМ включены процедуры уровня адаптации AAL5 и стандарта Q.2931. Обеспечение мультимедийных служб в АТМ позволило потребовать от сети предоставить пользователю при запросе на установление соединения обеспечение конкретных показателей качества обслуживания и согласовать показатели трафика. В сети Frame Relay показатели качества не используются, а число показателей трафика значительно меньше (CIR, Bc, Be)
- В АТМ предусмотрен в службе передачи данных сервис доступной битовой скорости ABR, позволяющей пользователям адаптировать их трафик к текущему состоянию сети. В сети Frame Relay такой экономически выгодный пользователю сервис не предусмотрен.
- Технология построения АТМ основывается на использовании первичных сетей связи с синхронной цифровой иерархией SDH, что позволяет передавать информацию по волоконно-оптическому кабелю на скоростях до нескольких терабит в секунду. В АТМ принята фиксированная длина ячейки и аппаратная реализация многих процедур. Сети Frame Relay работают на значительно меньших скоростях с использованием технологии цифровой иерархии PDH, имеющей недостатки по сравнению с SDH.
- Форум АТМ специализировал процедуру сигнализации на участке «пользователь-

сеть» и между коммутаторами сети. Протокол сигнализации PNNI между коммутаторами ATM предусматривает использование иерархической топологии сети, позволяющий создавать широкомасштабные сети. Технология Frame Relay не предусматривает создание широкомасштабной сети.

- В сети ATM предусмотрен стандартизированный протокол по выполнению функции маршрутизации по коррекции таблицы маршрутизации в зависимости от состояния каналов связи и узлов коммутации. В сети Frame Relay такой стандартизированный протокол отсутствует.
- На физическом уровне ATM один байт контрольно-проверочной комбинации циклического кода служит для исправления одиночных ошибок и обнаружения ошибок большей кратности четырех байт заголовка ячейки. Контрольно-проверочная комбинация поля данных ячейки ATM отсутствует. Протоколы адаптации ALL3/4 и ALL5 производят повторную передачу испорченных элементов CS-PDU, обеспечивая при этом высокий показатель QoS по вероятности потерь при службе передачи данных. В сети Frame Relay производится обнаружение ошибок поля данных без восстановления.

ГЛАВА 11. Первичные сети уплотненного волнового мультиплексирования

11.1. Основные функции DWDM

Технология уплотненного волнового мультиплексирования *DWDM (Dense Wave Division Multiplexing)* предназначена для создания оптических магистралей, работающих на терабитных скоростях. В отличие от технологии первичных сетей PDH и SDH, в которых для разделения высокоскоростного канала применяется временное мультиплексирование, а данные передаются в цифровой форме, сети DWDM не являются цифровыми. Сети DWDM предоставляют пользователям отдельные спектральные каналы, являющиеся несущей средой. Такой несущей средой DWDM является световая волна. Сети DWDM позволили существенно повысить пропускную способность современных телекоммуникационных сетей и организовать в одном оптическом волокне десятки волновых каналов, каждый из которых способен переносить цифровую информацию. Одно волокно может обеспечить скорость передачи до нескольких терабит в секунду. Таким образом, основными функциями DWDM являются операции мультиплексирования и демультиплексирования, т.е. объединение различных волн в одном световом пучке и выделение информации каждого спектрального канала из общего сигнала.

11.2. Принцип работы DWDM

Технология DWDM реализует частотное мультиплексирование световых волн, а не электрических как в системе FDM. Рисунок 11.1 иллюстрирует процесс DWDM. На вход DWDM каждый кадр STM синхронной цифровой иерархии SDH (см. глава 9) назначается для модуляции отдельному лазеру. Каждый лазер излучает сигнал на своей отличной от других длине волны λ (лямбда) в определенном диапазоне. В результате мультиплексирования выходные сигналы лазеров объединяются в одном оптическом волокне.

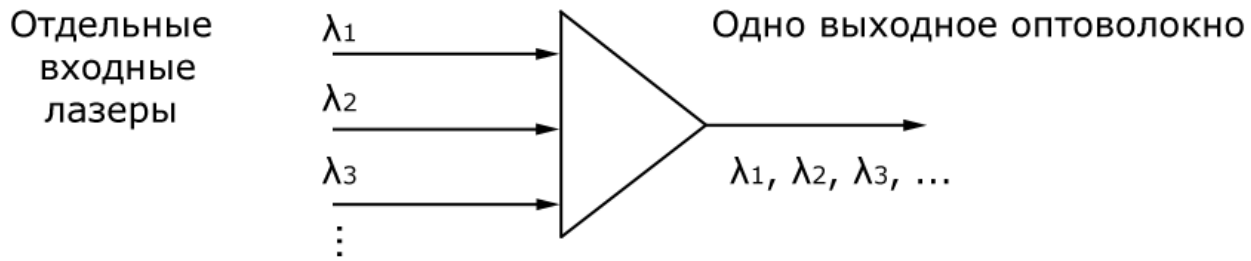


Рис. 11.1. Процесс мультиплексирования DWDM

У технологии DWDM имеется предшественница — технология волнового мультиплексирования WDM (Wave Division Multiplexing), которая использует от 2 до 16 спектральных каналов. По одному каналу переносится информация со скоростью до 10 Гбит/с. В системах DWDM может быть задействовано до 160 каналов на одном оптическом волокне, что обеспечивает скорости передачи данных для одного волокна до нескольких терабит в секунду. На рис. 11.2 показаны компоненты участка системы DWDM.

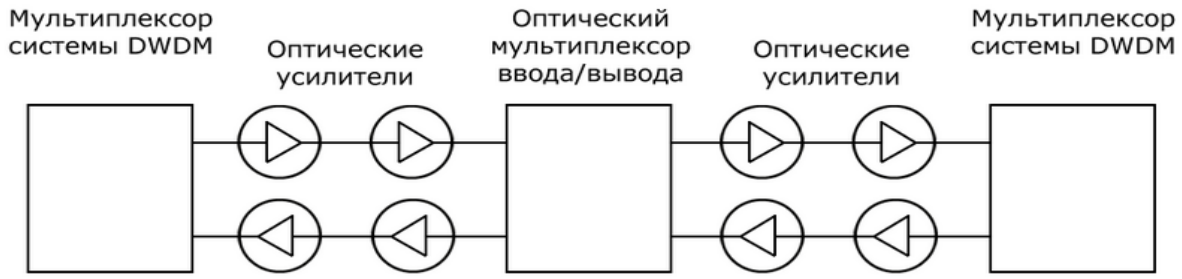


Рис. 11.2. Участок системы DWDM

На каждом конце участка находится терминальный мультиплексор системы DWDM. Этот мультиплексор обеспечивает распределение кадров синхронной цифровой иерархии SDH (или синхронной оптической сети SONET) по определенным длинам световых волн (λ), используемым для транспортировки. В тракт между терминальными мультиплексорами могут включаться оптические мультиплексоры ввода/вывода OADM (Optical Add/Drop Multiplexer). OADM поддерживает функции ввода/вывода на различных длинах волн. Вдоль участка на расстоянии порядка 150 км расположены оптические усилители. Хотя оптический усилитель восстанавливает мощность сигнала, он не полностью компенсирует (например, из-за распространения волн разной длины с разной скоростью). Поэтому для построения более

протяженных участков DWDM между определенным количеством участков с оптическими усилителями (до семи) устанавливаются мультиплексоры DWDM, выполняющие регенерацию сигнала путем её преобразования в электрическую форму и обратно. Технология DWDM в отличие от использования оптических волокон в SDH и Gigabit Ethernet (где световые сигналы всегда преобразуются в электрические перед мультиплексированием и коммутированием) между оптическими усилителями эти операции выполняются также над световыми сигналами.

Анализ сетевого трафика в течение последних двух десятилетий показывает на экспоненциальный рост его практически во всех регионах мира. Рост сетевого трафика вызывает постоянное увеличение спроса на пропускную способность технологии уплотненного волнового мультиплексирования DWDM (Dense Wave Division Multiplexing). DWDM работают на оптических магистралях на терабитных скоростях. По прогнозам к 2020 году скорость передачи по одному волокну в опорных сетях наиболее развитых стран приблизится к 20 Тбит/с [22].

На выставке «Связь Экспокомм-2012» российской компанией Т8 была представлена разработка 80 канальной системы DWDM со скоростью информации через каскад усилителей на 2000 км по каналу 100 Гбит/с. Максимальная емкость такой системы составляет 8 Тбит/с. Сегодня системы такого класса востребованы ОАО «Ростелеком» и другими крупными операторами. Оборудование по данным разработчиков обладает запасом по дальности передачи до 5-6 тысяч км. Показана передача по каналу 100 Гбит/с на 400км без промежуточных усилителей.

В настоящей разработке для десятикратного повышения канальной скорости (с 10 до 100 Гбит/с) и общей емкости системы (с 0,8 до 8 Тбит/с) использовался формат DP-QPSK [22]. В этом формате каждая из двух ортогональных поляризаций (DP) используется для передачи независимых потоков информации. В каждом из этих двух потоков информация передается с использованием 4-уровневой фазовой модуляции (QPSK). В результате скорость увеличивается в 4 раза (передается 4 бита на символ). В работе [22] отмечается, что увеличение канальной емкости позволяет уменьшить число каналов, а это упрощает управление сетью.

11.3. Типовые топологии

На рис. 11.3 приведена более полная схема двухточечного участка системы DWDM с вводом/выводом в промежуточных узлах OADM.

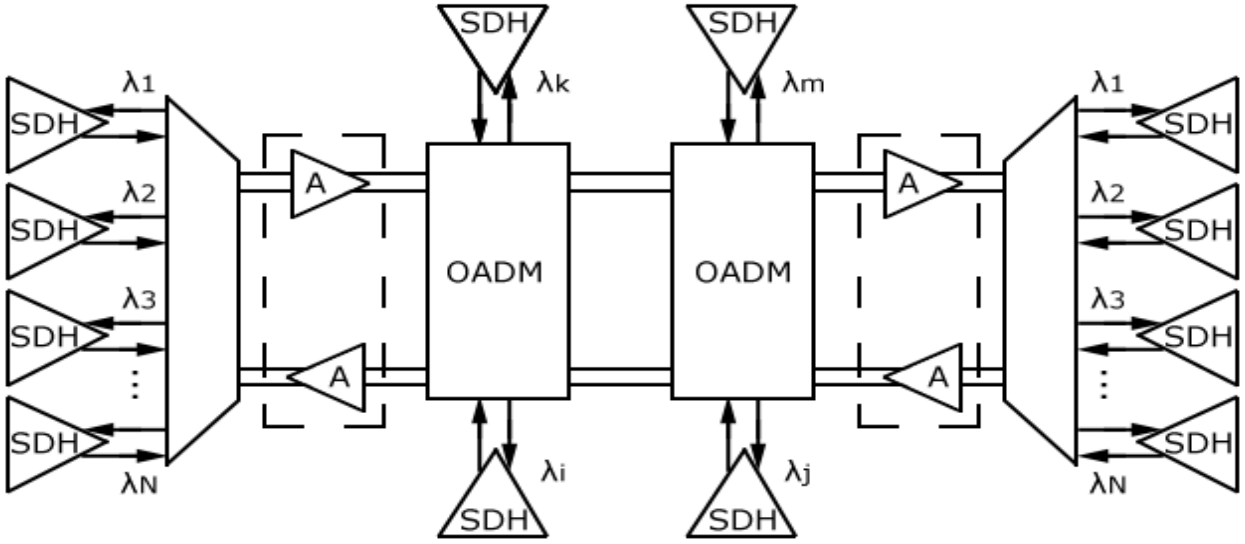


Рис. 11.3. Участок системы DWDM с вводом/выводом в промежуточных узлах

Оптические мультиплексоры ввода/вывода OADM могут вывести из общего оптического сигнала волну определенной длины и ввести туда сигнал этой же длины волны, так что спектр транзитного сигнала не изменится, а соединение будет выполнено с одним из абонентов, подключенных к промежуточному мультиплексору. OADM поддерживает операции ввода-вывода волн сугубо оптическими средствами или с промежуточным преобразованием в электрическую форму. Обычно полностью оптические (пассивные) мультиплексоры ввода-вывода могут отводить небольшое число волн, так как каждая операция вывода требует последовательного прохождения оптического сигнала через оптический фильтр, который вносит дополнительное затухание. Если же мультиплексор выполняет электрическую регенерацию сигнала, то количество выводимых волн может быть любым в пределах имеющегося набора волн, так как транзитный оптический сигнал предварительно полностью демультиплексируется.

Кольцевая топология сети (рис. 11.4) обеспечивает живучесть сети DWDM за счет резервных путей. Методы защиты трафика, применяемые в DWDM, аналогичны методам в SDH. Для того чтобы какое-либо соединение было защищено, между его конечными точками устанавливаются два пути: основной и резервный. Мультиплексор конечной точки сравнивает два сигнала и выбирает сигнал лучшего качества (или сигнал, заданный по умолчанию выводят их оттуда, как это делают мультиплексоры ввода-вывода, но и поддерживают произвольную коммутацию между оптическими сигналами, передаваемыми волнами разной длины.

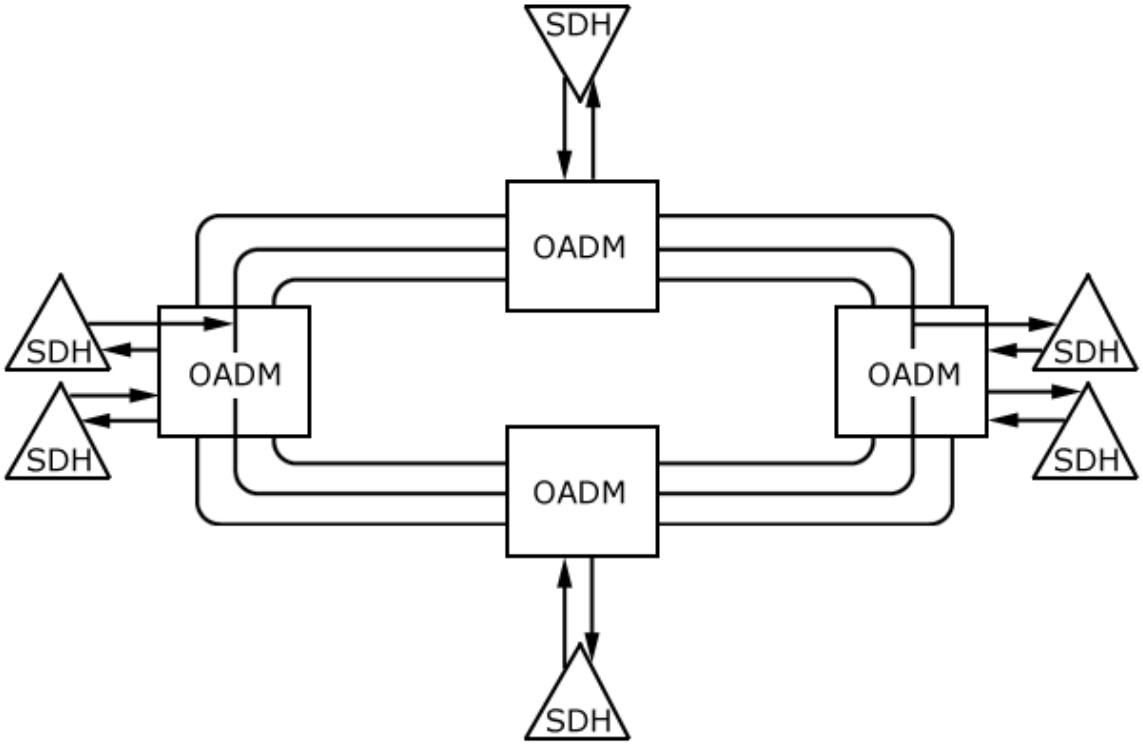


Рис. 11.4. Кольцо мультиплексоров DWDM

ГЛАВА 12. IP-сети. Стек протоколов TCP/IP и их функции

12.1. Стек протоколов TCP/IP

12.1.1. IP-сеть

IP-сеть (какой является Интернет**)** отличается от глобальных сетей тем, что является составной сетью из подсетей, число которых измеряется тысячами. Для Интернета характерно использование стека протоколов не эталонной модели OSI, а эталонной модели TCP/IP [10,23]. На рис. 12.1 представлен стек протоколов TCP/IP и его соответствие уровням модели OSI. Отличительной особенностью TCP/IP является также то, что IP-пакеты могут передаваться с использованием различных технологий составных сетей, в том числе посредством уже рассмотренных глобальных сетей X.25, FR и ATM, которые являются самостоятельными со своими протоколами, адресацией и др. Другой особенностью является то, что эталонная модель TCP/IP в отличие от эталонной модели OSI была разработана под конкретную составную сеть (интерсеть или internet). Подсети, составляющую эту составную сеть, соединяются между собой маршрутизаторами. Такими подсетями могут быть как локальные, так и глобальные сети различных технологий.

Прикладной уровень стека TCP/IP (уровень 4) соответствует трём верхним уровням модели OSI. К протоколам прикладного уровня относятся протокол переноса файлов (FTP); протокол электронной почты (SMTP); протокол передачи гипертекста HTTP (Hyper Text Transfer Protocol), используемый для создания страниц во всемирной паутине (глобальной гипертекстовой информационной системе) WWW (сокращенное название – web) - основа для доступа к связанным между собой документам; протокол преобразования (DNS) текстовых имен в сетевые IP-адреса, простой протокол сетевого управления (SNMP), протоколы соответственно сигнализации и передачи данных (SIP, RTP/RTCP) в IP-телефонии или речь поверх IP (VoIP-Voice over IP) и др. К протоколам прикладного уровня относятся также протоколы информационной безопасности Kerberos, PGP, SET и др.

Одним из наиболее распространенных протоколов прикладного уровня является протокол передачи гипертекста HTTP (Hyper Text Transfer Protocol). Для идентификации ресурсов (файлов) используется единообразный идентификатор ресурсов URI (Uniform Resource Identifier). Для определения местонахождения ресурсов в сети Интернет используются символьные адреса URL (Uniform Resource Locater). Всемирная паутина WWW представляет миллионы Web – серверов Интернет и клиентов во всем мире. Web –

сервер принимает по протоколу HTTP запрос от клиента на определенный ресурс. Сервер находит соответствующий файл и отправляет его запросившему компьютеру по тому же протоколу HTTP. Для просмотра полученной информации применяется программа Web – браузер.

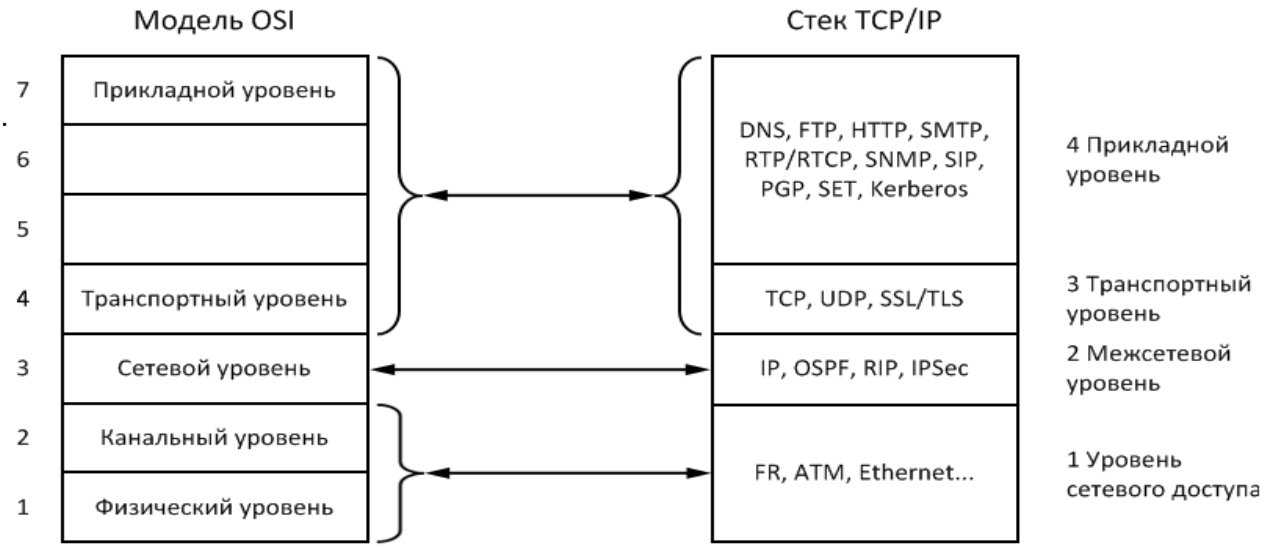


Рис. 12.1. Стек протоколов TCP/IP

В Интернете компьютеру присваивается многозначное числовое значение, называемое IP-адресом, и каждый IP-пакет содержит такой адрес получателя. Например, при десятичной записи IP-адрес содержит 12 разрядов. Пользователям тяжело запоминать такие адреса. Поэтому в Интернете пользователи используют символьные имена вместо IP-адресов. В Интернете на прикладном уровне предусмотрено преобразование этих имен, называемых доменными, в IP-адреса. Протокол преобразования называется службой имен доменов DNS (Domain Name System). В качестве средства передачи сообщений почтовая служба использует протокол прикладного уровня SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты). Большинство персональных компьютеров не могут получить сообщения напрямую. Вместо этого почтовый ящик пользователя физически находится на сервере, который постоянно готов к обработке и сохранению сообщений адресата. Адрес почтового ящика в Интернете состоит из двух символьных частей, разделенных между собой символом @. Первая часть адреса идентифицирует пользователя, а вторая показывает доменное имя компьютера, на котором находится его почтовый ящик.

12.1.2. Транспортный уровень стека TCP/IP

Транспортный уровень стека TCP/IP (уровень 3) обеспечивает передачу данных между

прикладными процессами. Транспортный уровень включает два протокола TCP и UDP. Протокол управления передачей TCP (Transmission Control Protocol) является надёжным протоколом с установлением соединения, позволяющим управлять потоком, т.е. без ошибок доставлять байтовый поток с одной машины на любую другую машину составной сети. Для того чтобы обеспечить надёжную доставку данных, протокол TCP предусматривает установление логического соединения. Это позволяет ему нумеровать пакеты, подтверждать их прием квитанциями, в случае потери организовывать повторные передачи, распознавать и уничтожать дубликаты, доставлять прикладному уровню в том порядке, в котором они были отправлены. Пакеты, поступающие на транспортный уровень, организуются в виде множества очередей к точкам входа прикладных процессов. В терминологии TCP/IP такие очереди, однозначно определяющие приложение в пределах хоста, называется портами. За портами каждого стандартного приложения определён номер, например, порт TCP № 21 - за протоколом передачи файла FTP (File Transport Protocol). Номер порта в совокупности с номером сети и номером конечного узла имеет название сокет (socket). Каждое логическое соединение идентифицируется парой сокетов взаимодействующих процессов. Второй протокол транспортного уровня - протокол пользователей дейтаграмм UDP (User Data Protocol) является простейшим дейтаграммным протоколом (т.е. без установления соединения). К протоколу транспортного уровня относится протокол информационной безопасности SSL/TLS. Протоколы прикладного и транспортного уровней стека уровней TCP/IP устанавливаются на оконечных станциях (хостах) сети.

12.1.3. Межсетевой уровень стека TCP/IP

Межсетевой уровень стека TCP/IP (уровень 2), называемый также сетевым уровнем (по модели OSI), является стержнем всей архитектуры TCP/IP. Именно этот уровень, функции которого соответствуют сетевому уровню модели OSI, обеспечивает перенос пакетов данных в пределах всей составной сети. Протоколы межсетевого уровня поддерживают интерфейсы с вышележащим транспортным уровнем, получая от него запросы на передачу данных по составной сети. Основным протоколом межсетевого уровня является межсетевой протокол IP (Internet Protocol). Он обеспечивает продвижение пакета между подсетями - от одного пограничного маршрутизатора до другого, до тех пор, пока пакет не попадёт в сеть назначения. Протокол IP так же, как и протоколы функций коммутации глобальных сетей связи (FR, ATM и др.), устанавливается не только на оконечных пунктах (хостах), но и на всех маршрутизаторах сети. Маршрутизатор представляет собой процессор, который связывает между собой две сети (подсети). Протокол межсетевого уровня работает в режиме без установления соединения (дейтаграммный

режим), в соответствии с которым он не отвечает за доставку пакета до узла назначения. При потере пакета в сети протокол IP не пытается восстановить его.

В заголовке IP-пакета содержится IP-адрес отправителя и получателя - по 4 байта каждый. К межсетевому уровню относятся также протоколы, выполняющие функции составления и коррекции таблиц маршрутизации RIP (Routing Internet Protocol), OSPF (Open Shortest Path First), протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). К протоколу сетевого уровня относится протокол информационной безопасности IPSec. Уровень сетевого доступа стека TCP/IP (уровень 1) отвечает за организацию интерфейса с частными технологиями подсетей составной сети. Перемещение пакета можно рассматривать как последовательность «прыжков» от одного маршрутизатора к другому. На очередном маршрутизаторе на сетевом уровне определяется сетевой адрес следующего по маршруту маршрутизатора. Чтобы передать пакет IP этому маршрутизатору, надо перенести его через некоторую подсеть. Для этого необходимо использовать транспортные средства этой подсети. Задача уровня сетевого доступа сводится к инкапсуляции (вложению) пакета в блок данных этой промежуточной сети и в преобразовании сетевых адресов граничных маршрутизаторов этой подсети в новый тип адреса, принятой в технологии промежуточной сети.

12.2. Пример переноса данных в IP-сети

На примере IP-сети (рис. 12.2) покажем перенос данных оконечной станции A локальной вычислительной сети (подсети) Ethernet в оконечную станцию B сети (подсети) ATM.

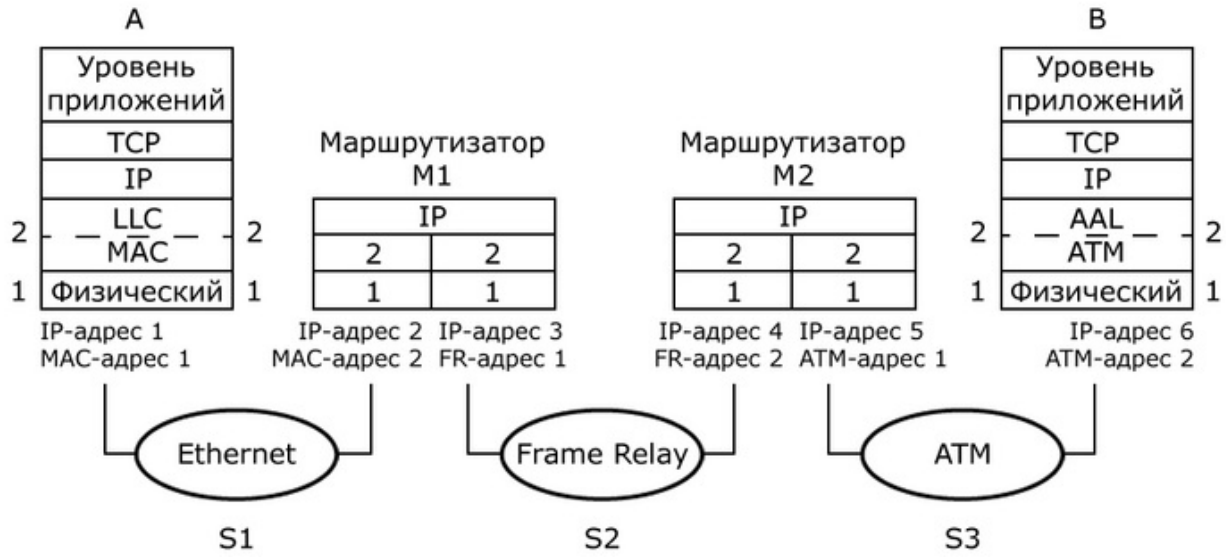


Рис. 12.2. Пример взаимодействия двух устройств

В основу приведенного упрощенного описания положен пример межсетевого взаимодействия сетей Ethernet и ATM, приведенный в работе [24]. Дополнительно в эту составную сеть введена сеть (подсеть) Frame Relay. Принцип маршрутизации и краткое описание протоколов маршрутизации в сети Интернет приведены в следующей главе.

Для того чтобы технология TCP/IP могла решать задачу объединения сетей, ей необходима собственная глобальная система адресации, не зависящая от способов адресации узлов в отдельных подсетях. Таким адресом является IP-адрес, состоящий из адреса подсети (префикса) и адреса оконечного устройства (хоста). Приведем пример адресации подсети и хоста. IP-адрес 200.15.45.126/25 означает, что 25 старших бит из выделенных 4-х байт под адресацию являются адресом подсети, а оставшиеся 7 бит означают адрес хоста в этой сети. Как видно из предыдущих глав, глобальные сети Frame Relay и ATM имеют различные системы нумерации, которые отличаются от системы нумерации локальной вычислительной сети (ЛВС) технологии Ethernet. Каждый компьютер Ethernet имеет уникальный физический адрес, состоящий из 48 бит. Этот адрес называется MAC-адресом и относится к канальному уровню — управлению доступом к среде MAC (Media Access Control). Для организации межсетевого взаимодействия подсетей различной технологии и адресации используются маршрутизаторы, включающие IP-пакеты. В состав этих пакетов входят глобальные IP-адреса. Каждый интерфейс маршрутизатора IP-сети и оконечного устройства включает два адреса – локальный адрес оконечного устройства подсети и IP-адрес.

Рассмотрим продвижение IP-пакета в составной сети (рис. 12.2).

1. Пользователь компьютера A сети Ethernet, имеющий IP-адрес(IP-адрес 1), обращается по протоколу передачи файла FTP к компьютеру B, подключенному к сети ATM и имеющий IP-адрес (IP-адрес 6).
2. Компьютер A формирует кадр Ethernet для отправки IP-пакета. По таблице маршрутизации в компьютере A на основании IP-адресов A и B определятся маршрутизатор M1 и входящий интерфейс для передачи этого IP-пакета. При этом становится известен IP-адрес интерфейса маршрутизатора M1(IP-адрес 2).
3. Компьютер A отправляет по сети Ethernet IP-пакет, инкапсулированный в кадр Ethernet и включающий следующие поля (рис. 12.3). MAC-адрес в заголовке кадра Ethernet занимает 6 байт. С помощью протокола разрешения адресов ARP (Address Resolution Protocol) определяются локальные адреса MAC-адрес 1 и MAC-адрес 2 по известным IP-адресам (IP-адрес 1 и IP-адрес 2).

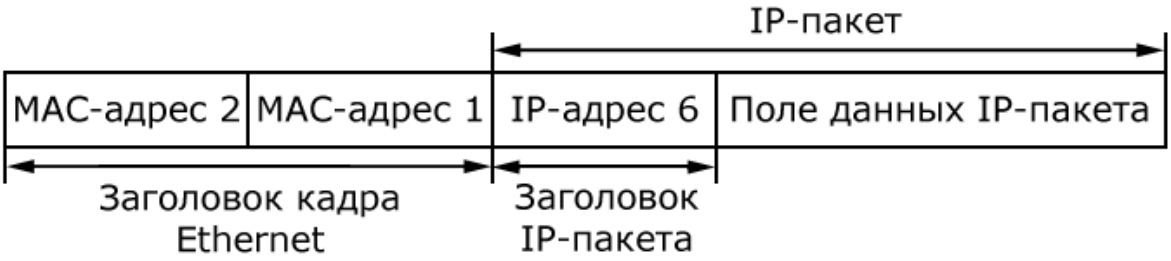


Рис. 12.3. Кадр Ethernet с инкапсулированным в него IP-пакетом

4. Кадр принимается на входном интерфейсе маршрутизатора М1 в соответствии с протоколом Ethernet. Протокол Ethernet извлекает из принятого кадра IP-пакет, инкапсулированный в него. Из этого IP-пакета маршрутизатор М1 извлекает IP-адрес назначения (IP-адрес 6).
5. С помощью таблицы маршрутизации в М1 определяются IP-адреса выходного интерфейса из М1 и входного интерфейса маршрутизатора М2, т.е. IP-адрес 3 и IP-адрес 4.
6. По глобальным адресам IP-адрес 3 и IP-адрес 4 определяются соответственно локальные адреса подсети Frame Relay FR-адрес 1 и FR-адрес 2.
7. IP-пакет передается по виртуальному каналу сети Frame Relay, используя при этом локальные адреса FR-адрес 1 и FR-адрес 2. Этот IP-пакет инкапсулирован в кадр FR.
8. Кадр FR принимается на входном интерфейсе маршрутизатора М2 в соответствии с протоколом сети Frame Relay. Извлекается принятый IP-пакет, сбросив заголовок принятого кадра FR. Извлекается IP-адрес назначения (IP-адрес 6).
9. С помощью таблицы маршрутизации в М2 определяется IP-адреса выходного интерфейса (IP-адрес 5) маршрутизатора М2 и IP-адрес назначения (IP-адрес 6). При этом глобальным адресам определяются соответствующие им локальные адреса ATM-адрес 1 и ATM-адрес 2. IP-пакет передается по виртуальному каналу сети ATM, используя эти локальные адреса.
10. В результате IP-пакет из компьютера А поступает в компьютер В.

12.3. Протоколы TCP/IP

Ниже приводится краткое описание протокола прикладного уровня SNMP и протокола транспортного уровня TCP архитектуры TCP/IP.

12.3.1. Протокол прикладного уровня SNMP

Большие сети не могут быть настроены и управляться вручную в плане изменения

конфигурации сети, устранения неисправности в сети, сбора параметров о качестве обслуживания. Если в сети используется оборудование разных производителей, необходимость таких средств становится особенно необходимой. В связи с этим были разработаны стандарты сетевого управления. Одним из наиболее широко используемых является простой протокол управления сетью SNMP (Simple Network Management Protocol) [9]. Приведем краткие сведения об архитектуре сетевого управления.

Система сетевого управления включает инструментальные средства для решения задач управления. При этом необходимо использование уже имеющегося оборудования путем внедрения в него дополнительных аппаратных и программных средств для управления сетью. Это программное обеспечение размещается в хостах, коммуникационных процессорах и других устройствах сети. Модель сетевого управления, используемая для SNMP, состоит из следующих элементов:

- станция управления, выполняющая роль интерфейса между сетевым администратором и системой сетевого управления. Станция управления позволяет осуществить мониторинг сети и управление сетью. В этой станции имеется база данных с информацией, полученной из информационных баз всех управляемых объектов сети;
- агент управления (хосты, коммутаторы и др.), которые отвечают на запросы от станции управления. Агент обеспечивает информацией станцию и без запроса;
- агент поддерживает базу данных, именуемую MIB (база управляющей информации, Management Information Base), в которой записаны конфигурация, характеристики и состояние устройств.

Станция управления и агенты взаимодействуют по протоколу SNMP.

Так как управление сетью задача многоцелевая, приведем некоторые возможности использования протокола SNMP в сети Frame Relay [15]. Форум Frame Relay стандартизировал MIB для устройств Frame Relay. В большинстве служб Frame Relay провайдер собирает информации от агентов SNMP в каждом коммутаторе FR и записывает ее в центральную базу MIB для общего пользования. Тем самым пользователю предоставляется единый источник статистической информации обо всех соединениях виртуальных каналов сети. Это дает возможность отследить свои потоки данных в сети провайдера от коммутатора к коммутатору. Можно использовать SNMP для сбора статистики и аварийных сообщений от собственного оборудования, подключенного к сети FR. Для этого приходится работать с множеством MIB. Для сбора данных на основе SNMP можно использовать виртуальный

канал FR. SNMP может управлять конфигурацией сети. Для сети FR это касается как физической, так и логической конфигурации сети, включая установление адресации, определение DLCI, назначение полосы пропускания для PVC. SNMP может управлять устранением неисправностей в сети при получении системой управления аварийных сообщений от агента сетевого устройства.

Обеспечение информационной безопасности протокола SNMP

В документе RFC 2574 [25] определяется модель USM (User Security Model – модель защиты пользователя) при использовании протокола SNMP. USM разрабатывалась с целью защиты от угроз следующих типов.

- *Модификация информации.* По пути следования сообщения, сгенерированного авторизованным объектом, некоторый другой объект может изменить это сообщение, чтобы выполнить несанкционированные операции управления (например, установив соответствующие значения объекта управления). Суть угрозы заключается в том, что несанкционированный объект может изменить любые параметры управления, включая параметры конфигурации, выполняемых действий и контроля.
- *Имитация.* Объект может пытаться выполнить не разрешенные для него операции управления, отождествляя данный объект с некоторым авторизованным объектом.
- *Модификация потока сообщений.* Протокол SNMP предназначен для работы над транспортным протоколом, не предполагающим установку соединений. Существует угроза переупорядочения, задержки или воспроизведения (дублирования) сообщений SNMP для несанкционированного управления. Например, можно скопировать и впоследствии воспроизвести сообщение, вызывающее перезапуск устройства.
- *Разглашение информации.* Наблюдая за потоком обмена данными между администратором и агентом, объект может выяснить значения управляемых объектов и распознать подлежащие регистрации события. Например, наблюдение за набором команд, изменяющих пароли, может позволить атакующему узнать новые пароли.

12.3.2. Протокол транспортного уровня TCP

Протокол транспортного уровня TCP выполняет функцию управления потоками между оконечными пунктами, так как уровень IP не гарантирует правильной доставки дейтаграмм. Дейтаграммы с уровня IP могут прибывать в неправильном порядке. Восстанавливает сообщения из таких дейтаграмм протокол TCP, обеспечивая этим надежный

режим установленного соединения с низкой вероятностью потери пакета. Механизм управления потоками, используемый TCP, отличается от механизма восстановления правильной последовательности кадров в X.25 и называется схемой кредитов. В этой схеме считается, что каждый передаваемый байт данных имеет порядковый номер. Границы между сообщениями не сохраняются. Например, если отправляющий прикладной процесс записывает в TCP-поток четыре 512-байтовые порции данных, эти данные могут быть доставлены получающему процессу в виде четырех 512-байтовых порций, либо двух 1024-байтовых порций, либо одной 2048-байтовой порции. Каждая протокольная единица PDU TCP называется сегментом TCP и включает в заголовок сегмента порт источника данных и порт получателя. Значения портов идентифицируют соответствующих пользователей (приложения) двух объектов TCP. Логическая связь относится именно к данной паре значения портов. В процессе связи каждый объект отслеживает сегменты TCP, получаемые от другой стороны или отправленные другой стороне, для того, чтобы регулировать поток сегментов и восстанавливать утерянные или поврежденные сегменты. Стандартный номер порта однозначно идентифицирует тип приложения, однако он не может однозначно идентифицировать прикладной процесс этого приложения. Одно приложение может одновременно осуществлять несколько процессов. Поэтому прикладной процесс однозначно определяется в пределах сети и в пределах отдельного компьютера парой (IP-адрес, номер порта) и называется сокетом (socket). Логическое TCP-соединение однозначно идентифицируется парой сокетов, определенных для этого соединения двумя взаимодействующими сокетами. При работе на хост-отправителе протокол TCP рассматривает информацию, поступающую к нему от уровня приложений, как неструктурированный поток байтов. Эти данные буферируются средствами TCP. На уровень IP из буфера «вырезаются» сегменты, к которым добавляются заголовки. В состав заголовка входят сегменты SYN и ACK, служащие для установления TCP-соединения. Для передачи сегмента данных имеются три поля, связанные с управлением потоком (восстановлением целостности принятого сообщения): *порядковый номер (SN), номер подтверждения (AN) и окно (W)*.Когда транспортный объект отправляет сегмент, он помещает в поле данных сегмента порядковый номер первого байта. Принимающий объект подтверждает получение сегмента с помощью обратного сегмента, в котором (AN=i, W=j), что означает:

- все байты до SN=i-1 подтверждены. Следующий ожидаемый байт имеет номер AN=i.
- разрешается отправить дополнительное окно из W=j байт данных, т.е. байты от I до i+j-1.

Таким образом, протокол TCP обеспечивает надежную доставку сообщений, поступающих из сети от ненадежного дейтаграммного протокола на межсетевом уровне. В сети X.25 функцию надежной доставки выполняет канальный уровень модели OSI, который был подробно рассмотрен в предыдущих главах, а в сети Frame Relay эту функцию выполняет протокол ITU-T Q.921.

ГЛАВА 13. IP-сети. Межсетевой уровень. Протоколы безопасности

13.1. Протоколы межсетевого уровня

13.1.1. Формат IP-пакета

Основным протоколом межсетевого уровня является протокол IP (Internet Protocol). IP - протокол выполняет функцию продвижения пакета между подсетями. Формат IP-пакета включает поле заголовка этого пакета и поле полезного груза. Под полезным грузом понимается поле, включающее заголовок сообщения транспортного уровня и данные прикладного уровня. В отличие от протоколов прикладного и транспортного уровней протокол IP устанавливается не только на оконечных станциях, но и на всех маршрутизаторах сети. IP - протокол является дейтаграммным ненадежным (без подтверждения) протоколом без установления соединений, т.е. дейтаграммным (гл. 2, разд. 2.2). Термин “ненадежный” отражает тот факт, что протокол IP не делает ничего, чтобы гарантировать доставку пакета, гарантировать последовательность доставленных пакетов, нет подтверждений, нет контроля ошибок и управления потоками данных. Если пакеты потеряны, то оконечному пункту (хосту) об этом не сообщается, а решением этой проблемы должны заниматься более высокие уровни.

Протокол IP реализует сеть передачи дейтаграмм. Дейтаграмма – это общее название для единиц данных, которыми оперируют протоколы без установления соединения. Дейтаграмму протокола IP называют также пакетом. Для доставки пакета протокол IP использует иерархическое структурирование IP – адресов, контроль за временем жизни пакетов в сети и проверку целостности заголовка IP – пакета. Как протокол без установления соединения, протокол IP обрабатывает каждую дейтаграмму индивидуально, т.е. каждый пакет маршрутизируется индивидуально. Узлы сети не устанавливают логическое соединение перед обменом IP – пакетами.

IP-пакет состоит из заголовка и инкапсулированного сегмента транспортного уровня. Приведём некоторые поля заголовка пакета IP.

Поле протокола верхнего уровня содержит идентификатор, указывающий какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета. Например, 6 означает, что в пакете находится заголовок протокола TCP, 17 - протокола UDP.

Поле IP - адресов источника и приемника имеют одинаковую длину 4 байта. IP-адреса

представляются в формате десятичного представления с разделительными точками, где каждый байт представляется своим десятичным эквивалентом. Эти четыре десятичных числа разделяются точкой (например, 128.67.38.255). Каждый IP-адреса состоит из двух частей: идентификатора сети (подсети) NETID (network identifier) и идентификатора хоста HOSTID (host identifier). NETID идентифицирует определенную сеть, к которой подключен хост.

Маршрутизаторы используют только NETID, который иногда называют префиксом сети. IP-адрес 128.67.38.255 имеет идентификатор сети 128.67 (в двоичном виде третий и четвертый байты – 10000000 и 01000011) и идентификатор хоста 38.255 (в двоичном виде первый и второй байты – 00100110 11111111). В протоколе IP для извлечения идентификатора сети NETID используется маска с использованием слэша (/). В маске каждый бит, которой является частью идентификатора сети NETID, равен 1, а биты, являющиеся частью идентификатора хоста HOSTID, равны 0. Например, 128.67.38.255/16 означает, что первые 16 битов этого адреса – это идентификатор NETID 128.67.0.0. За счет управления битами в маске группа IP-адресов может быть разбита на меньшие сети. Например, добавив 3 бита к 24 разрядной маске сети 3 бита, добавляется 8 новых сетей, каждая из которых содержит меньшее количество идентификаторов хостов.

Для идентификации компьютеров в IP-сетях используют IP-адреса. Однако пользователи пользуются более удобными символьными именами компьютеров. Символьные идентификаторы строятся по иерархическому принципу. Составляющие символьного (или доменного) имени разделяется точкой и перечисляются в следующем порядке: сначала простое имя хоста, затем имя группы хостов (например, имя организации), потом имя более крупной группы (домена) и так далее до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: RU – Россия, UK – Великобритания). Вместо отправки электронной почты на адрес Alla@128.67.38.255 удобнее выглядит адрес: Alla@art.edu.ru. Для преобразования текстовых имен была разработана служба имен доменов DNS (Domain Name System). Для преобразования имени в IP-адрес программа прикладного уровня обращается к процедуре распознавателя, который посылает UDP-пакет DNS-серверу. Этот сервер находит имя в базе данных и возвращает соответствующий IP-адрес вызвавшей его программе прикладного уровня.

- Поле общей длины IP - пакета (т.е. заголовка и данных).
- Поле время жизни**.** Определяет, как долго дейтаграмма может оставаться в сети. Каждый маршрутизатор уменьшает значение поля, как минимум, на единицу. Поэтому поле является механизмом самоуничтожения пакета.

- Контрольная сумма циклического кода заголовка (контрольно-проверочная комбинация КПК) занимает 2 байта и рассчитывается только по заголовку.

Поскольку некоторые поля заголовка могут изменяться (например, время жизни), это поле проверяется на каждом маршрутизаторе. Если контрольная сумма неверна, то пакет отбрасывается, как только обнаруживается ошибка.

13.1.2. Принцип маршрутизации

Важнейшей задачей сетевого уровня является маршрутизация — передача пакетов между двумя конечными узлами в составной сети Интернет (т.е. интерсети-internet). Каждую из этих сетей часто называют подсетью. Рассмотрим принципы маршрутизации на примере небольшого фрагмента составной сети (рис. 13.1). В этой части сети несколько маршрутизаторов (M7, M9, M10, M14) объединяют несколько подсетей (S2, S3, S5, S8, S6). Маршрутизатор имеет несколько портов (минимум два), к которым присоединяются подсети. Каждый порт маршрутизатора можно рассматривать как отдельный узел сети: он имеет собственный сетевой адрес и собственный локальный адрес в той подсети, которая к нему подключена. Например, маршрутизатор под номером 14 имеет два порта, к которым подключены подсети S2 и S5. Сетевые адреса этих портов обозначены как M14(1) и M14(2). Порт M14(1) имеет локальный адрес в подсети с номером S2, порт M14(2) - в подсети S5. Таким образом, маршрутизатор можно рассматривать как совокупность нескольких узлов, каждый из которых входит в свою сеть.

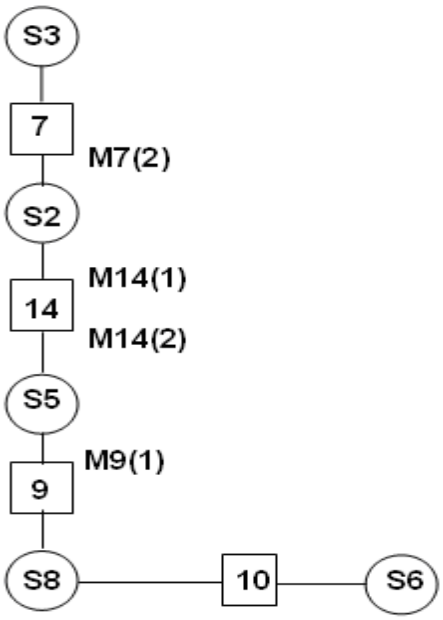


Рис. 13.1. Маршрутизация в сети Интернет

В сложных составных сетях почти всегда существует несколько маршрутов для передачи пакетов между двумя конечными узлами. Маршрут - это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до получателя. Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также на основании указанного критерия выбора маршрута (метрики). Примером такой метрики может быть количество пройденных в маршруте промежуточных маршрутизаторов (хопов). Чтобы по адресу сети назначения можно было выбрать рациональный маршрут дальнейшего следования пакета, каждый конечный узел и маршрутизатор анализируют специальную информационную структуру, которая называется таблицей маршрутизации.

Посмотрим, как могла бы выглядеть таблица маршрутизации, например, в маршрутизаторе 14 (табл. 13.1).

Таблица 13.1. Таблица маршрутизации в М14

Номер сети назначения	**Сетевой адрес следующего маршрутизатора**	**Сетевой адрес выходного порта**	**Расстояние до сети назначения**
S2	-	M14(1)	0
S3	M7(2)	M14(1)	1
S5	-	M14(2)	0
S6	M9(1)	M14(2)	2

В первом столбце таблицы перечисляются номера сетей, входящих в интерсеть и которые являются сетями назначения данного IP-пакета. В каждой строке таблицы следом за номером подсети указывается сетевой адрес следующего маршрутизатора (более точно, сетевой адрес соответствующего порта следующего маршрутизатора), на который надо направить пакет, чтобы тот передвигался по направлению к сети с данным номером по рациональному маршруту. Когда на маршрутизатор поступает новый пакет, номер сети назначения (профиль сети), извлеченный из поступившего кадра, последовательно сравнивается с номерами сетей в строках таблицы. Строка с совпавшим номером сети указывает, на какой ближайший маршрутизатор следует направить пакет. Например, если на порт маршрутизатора 14 поступает пакет, адресованный в сеть S6, то из таблицы маршрутизации маршрутизатора 14 следует, что сетевой адрес следующего маршрутизатора — M9(1), то есть очередным этапом движения данного пакета будет движение к порту 1 маршрутизатора 9. Сетевой адрес выходного порта – M14(2). Из приведенной таблицы следует, что IP-пакет поступает в подсеть назначения S6 через подсеть S5. В четвёртом столбце таблицы маршрутизации маршрутизатора 14 указано расстояние до подсети назначения в хопах (число промежуточных маршрутизаторов), которое равно 2. Если на порт маршрутизатора 14 поступает пакет, адресованный в сеть S3, то из таблицы маршрутизации маршрутизатора 14 следует, что сетевой адрес следующего маршрутизатора — M7(2), то есть очередным этапом движения данного пакета будет движение к порту 2 маршрутизатора 7. Сетевой адрес выходного порта – M14(1). Из приведенной таблицы следует, что IP-пакет поступает в подсеть назначения S3 через сеть S5. В четвёртом столбце таблицы маршрутизации маршрутизатора 14 указано расстояние до сети назначения в хопах, равное 1.

13.1.3. Внутренние и внешний протоколы маршрутизации

Для рассмотрения протоколов маршрутизации необходимо ввести понятие автономной системы. Автономная система AS (Autonomous System) обладает следующими признаками:

1. AS – это множество маршрутизаторов и сетей (подсетей), управляемых одной организацией.
2. AS состоит из группы маршрутизаторов, обменивающихся информацией через общий протокол маршрутизации.
3. За исключением состояния неисправности в AS существует путь между любой парой узлов.

На рис. 13.2 приведена IP – сеть, состоящая из двух AS. Протокол маршрутизации, который передаёт информацию между маршрутизаторами внутри AS, называется внутренним протоколом маршрутизации IRP (Interior Routing Protocol). При этом алгоритмы маршрутизации, используемые маршрутизаторами различных AS, могут отличаться. Тем не менее, маршрутизаторы в одной AS должны иметь минимальный уровень информации, связанной с сетями других AS, на которые возможна отправка пакетов. Протокол, который используется для передачи информации между маршрутизаторами в различных AS, называется внешним протоколом маршрутизации ERP (Exterior Routing Protocol).

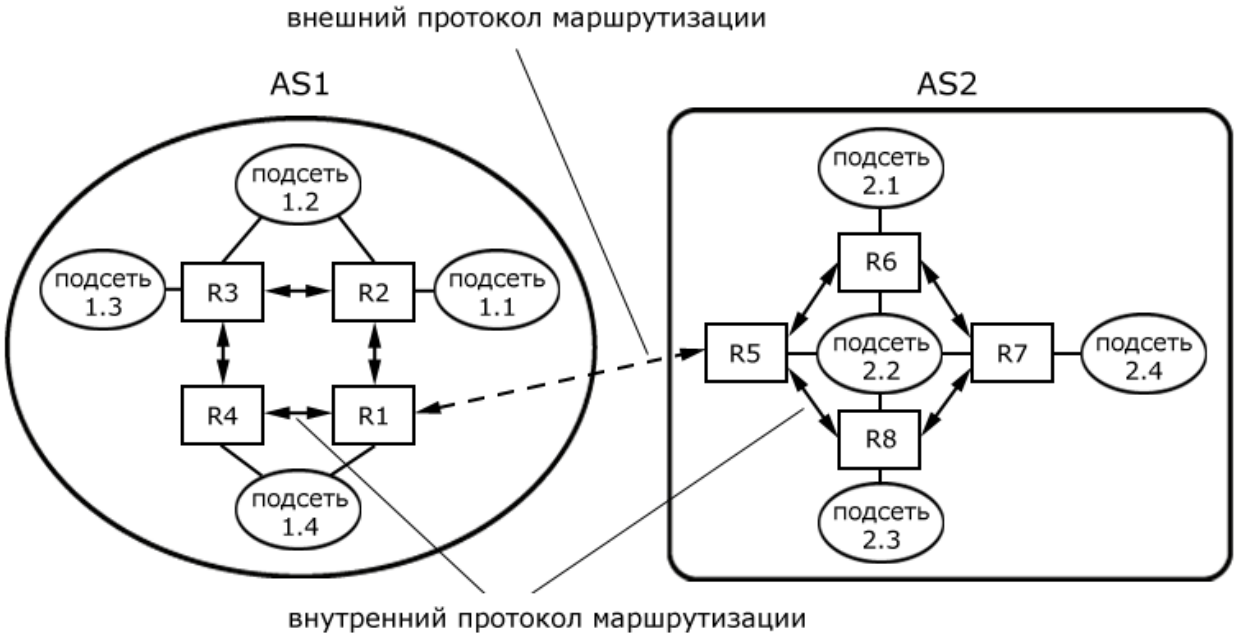


Рис. 13.2. Внутренний и внешний протоколы маршрутизации

Приведём краткое описание внутренних протоколов RIP и OSPF, а также внешнего протокола маршрутизации BGP. Протоколы RIP и OSPF входят в состав межсетевого уровня

архитектуры TCP/IP и выполняют две функции:

- построение таблицы маршрутизации;
- обновление таблиц маршрутизации, если состояние связей в составной сети изменилось по причине изменения топологии сети (отказа каналов связи, перегрузки и др.).

13.1.3.1. Протокол RIP

Протокол маршрутной информации RIP (Routing Information Protocol) является внутренним протоколом маршрутизации дистанционно-векторного типа. Определенный в документе RFC 1058 в качестве метрики протокол RIP использует число транзитных маршрутизаторов (хопов). Согласно спецификации, маршрутизатор извлекает информацию о подсети и расстоянии из своей таблицы маршрутизации и передаёт эти данные соседним маршрутам через каждые 30 секунд. Соседний узел, в свою очередь передает информацию соседнему узлу, пока все узлы внутри сети не получат одинаковую информацию о маршрутах. Протокол RIP продолжает оставаться популярным протоколом маршрутизации, поскольку он прост и хорошо подходит для небольших IP-сетей. Однако он имеет множество ограничений, включая следующие.

- RIP неприемлем для больших конфигураций (более 15 подсетей). Если разрешить метрики большого размера, то чрезмерно увеличится время формирования таблиц маршрутизации или их коррекции после изменения топологии. Способ обмена таблицами маршрутизации, принятый протоколом RIP, в крупных сетях может привести к перегрузке сети.
- В современных сетях использование числа транзитов в качестве метрики маршрутизации не всегда эффективно, т.к. она не берёт в расчёт загрузку каналов передачи, не учитывает разную пропускную способность каналов. Протокол RIP выбирает маршрут через два маршрутизатора через каналы 64Кбит/с, хотя мог бы быть выбран более экономичный маршрут через три маршрутизатора через каналы 2,048 Мбит/с. Этот экономичный выбор обеспечивает протокол OSPF.

13.1.3.2. Протокол OSPF

Протокол маршрутизации - OSPF (Open Shortest Path First - выбор кратчайшего пути первым) использует принцип контроля состояния канала, а метрика представляет собой оценку эффективности связи в этом канале. Чем меньше метрика, тем эффективней организация связи. Метрика, оценивающая пропускную способность канала, определяется, например, компанией Cisco, как количество секунд для передачи 100Мбит. Тогда, например,

- канал типа E1 = 2,048 Мбит/с (глава 3) соответствует метрике 488;
- канал 64 Кбит/с соответствует метрике 1562.

В этом случае маршрут через три маршрутизатора с каналами типа E1 составит метрику 488+488=976 единиц и является более экономичным по сравнению с маршрутом между двумя маршрутизаторами с каналом 64 Кбит/с (метрика 1562).

При первоначальном построении таблицы маршрутизации маршрутизатор определяет метрику канала на каждом своём интерфейсе. Затем маршрутизатор информирует об этих значениях все другие маршрутизаторы сети. На основании этих данных каждый маршрутизатор строит топографическую карту (базу данных) сети, по которой определяется кратчайший путь к каждой подсети. Данные этих кратчайших маршрутов помещаются в таблицу маршрутизации маршрутизатора. При невозможности передать пакеты к сети назначения (из-за отказа каналов связи, транзитных маршрутизаторов, перегрузках и др.) эти пакеты отбрасываются. Каждая запись в топологической базе данных сети имеет свой срок жизни. С каждой записью связан таймер, который служит для контроля времени жизни записи. Если какая-либо запись в топологической базе данных устаревает, то первый из таких маршрутизаторов запрашивает её новую копию с помощью специального пакета OSPF "Запрос сведений о состоянии каналов" (Link-State Request), на который должен поступить ответ "Корректировка сведений о состоянии каналов" (Link-State Update) или "Уведомление о состоянии канала" (Link-State Acknowledgement) от маршрутизатора непосредственно тестирующего эту связь. Если состояние связей в сети изменилось и произошла корректировка в маршрутизаторе сети, то этот маршрутизатор в широковещательном режиме сообщает всем соседним маршрутизаторам эти изменения. В OSPF передается только часть таблицы маршрутизации, а не вся таблица маршрутизации, как в RIP.

13.1.3.3. Протокол BGP

Основа работы протокола внешней маршрутизации BGP (Border Gateway Protocol - пограничный шлюзовой протокол) обмен маршрутной информации между

маршрутизаторами в нескольких автономных системах AS. Рассмотрим его работу на примере IP-сети из двух AS (рис 13.2). Вначале на маршрутизаторе R1 в AS1 реализуется внутренний протокол маршрутизации, например OSPF. В результате создаётся таблица маршрутизации в R1. Затем по протоколу TCP (порт 179) R1 посылает сообщение Update на маршрутизатор R5 в AS2. В это сообщение включена следующая информация:

1. идентификатор AS1;
2. IP - адрес маршрутизатора R1;
3. список всех подсетей в AS1, достижимых через R1.

Допустим, что R5 имеет также связь с другим маршрутизатором в другой AS, например, с маршрутизатором R9 в AS3. Маршрутизатор R5 будет передавать информацию, полученную от R1, в R9 в новом сообщении Update. В это сообщение включена следующая информация:

- список идентификаторов (AS1, AS2);
- IP - адрес маршрутизатора R5;
- список всех подсетей в AS1.

Это сообщение информирует маршрутизатор R9 о том, что все подсети AS1 достижимы через R5 и пересекаемыми автономными системами являются AS1 и AS2. Маршрутизатор теперь должен принять решение, является ли этот маршрут к перечисленным подсетям предпочтительным. Он может иметь альтернативные маршруты к некоторым или ко всем этим подсетям, которые по некоторым показателям (производительность, некоторые метрики и др.) сочтёт более предпочтительными. В таком случае R9 присоединяет эту информацию к своей и передаёт список всех подсетей AS1, AS2. Обновлённая таким образом информация распространяется по Интернету, который состоит из большого числа взаимодействующих AS.

13.2. Протоколы информационной безопасности

Прежде, чем перейти к описанию протоколов информационной безопасности сетей связи в настоящей и последующих главах следует изучить приведенные в приложении А общие положения архитектуры сетевой безопасности. Общие положения архитектуры сетевой безопасности изложены в рекомендации международного союза электросвязи ITU-T (International Telecommunication Union – Telecommunication) X.805 [26]. Эта рекомендация закладывает основы для разработки общих и детальных рекомендаций по этим вопросам для конкретных сетей независимо от их технологии и соответствия эталонным моделям OSI или TCP/IP. При изложении материала настоящей работы термин «сетевая безопасность» часто будет заменён широко используемым в литературе равнозначным ему термином «информационная безопасность в сетях» или в данной работе просто «информационная безопасность» (ИБ). Под угрозой согласно рекомендации ITU-T X.800 [27] понимается потенциальная возможность нарушения безопасности.
Ниже кратко изложены принципы выполнения функций протоколами информационной безопасности на прикладном уровне (протокол PGP), на транспортном уровне (протокол TLS), на межсетевом уровне (протокол IPSec).

13.2.1. Протокол прикладного уровня PGP

Настоящий раздел посвящен описанию принципов работы протокола информационной безопасности электронной почты PGP (Pretty Good Privacy). Согласно приведенному в разделе «Введение» этот протокол прикладного уровня, который не относится к сети связи (он принадлежит к инфокоммуникационной сети). Краткое изложение PGP в настоящем разделе преследует цель упрощения описания других протоколов ИБ, относящихся к сетям связи. Прежде, чем перейти к PGP следует ознакомиться с приложением В (Шифрование с открытым ключом). Более детальное описание этих алгоритмов, учитывающее требования к ключам шифрования, приводится в приложении Е.

Протокол PGP представляет собой полный пакет для электронной почты, обеспечивающий конфиденциальность сообщений, аутентификацию (подлинность источника сообщения и целостность сообщения с помощью цифровой подписи). В настоящем разделе приводится краткое описание этих алгоритмов. Хотя протокол PGP

относится к прикладному уровню (который не выполняет функции сетей связи) анализ в настоящем разделе этих алгоритмов безопасности служит только для понимания алгоритмов безопасности, используемых в сетях связи. На примере использования одного из наиболее распространенных алгоритмов асимметричной криптографии, называемого RSA, покажем шифрование/дешифрование сообщений и аутентификацию сообщений.

Шифрование/дешифрование сообщений по протоколу PGP приведено на рис. 13.3.

Сообщение M шифруется общим (сеансовым) ключом Ks с помощью традиционной симметричной криптографии. Этот ключ генерируется на стороне абонента A и шифруется открытым ключом абонента B. Шифрование производится асимметричной криптографией EP с помощью открытого ключа Eв получателя сообщения. Зашифрованный общий ключ $E_B(Ks)$ (который иногда называют цифровым конвертом) и зашифрованное этим ключом сообщение C=Ks(M) передается по каналам связи сети абоненту B.

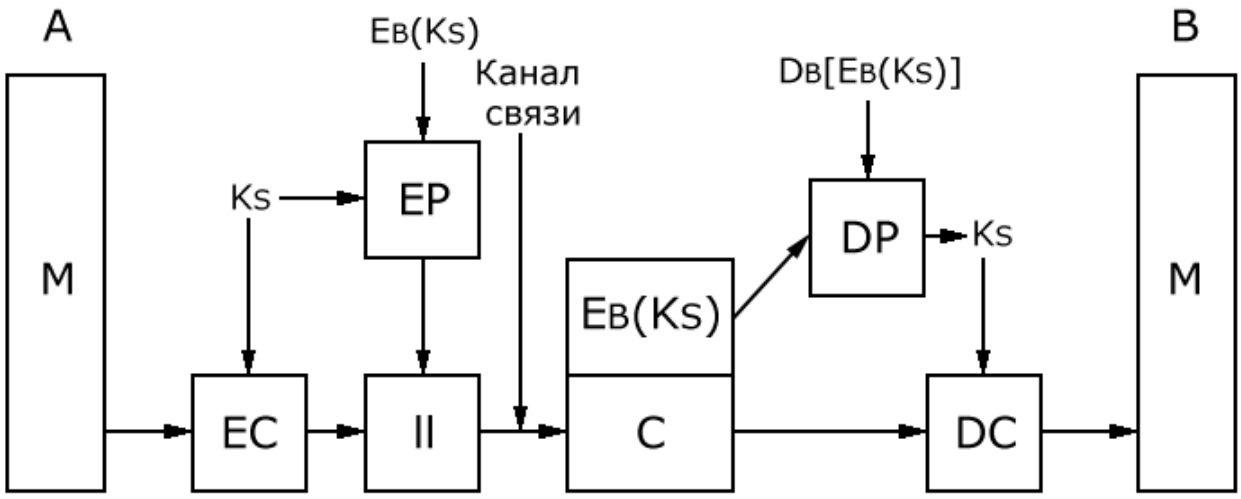


Рис. 13.3 Шифрование/дешифрование сообщений

На стороне абонента B с помощью его закрытого ключа Dв производится дешифрование DP. В результате получаем ключ симметричного шифрования Ks=Dв[E_B(Ks)], отправленный зашифрованным на стороне абонента A. Этим ключом производится дешифрование DC зашифрованного сообщения M (т.е. C=Ks(M)) с помощью симметричной криптографии с общим ключом.

Аутентификация сообщения протоколом PGP выполняется с помощью цифровой подписи с использованием криптографии с открытым ключом и профиля сообщения. Для создания цифровой подписи выполняется следующая последовательность действий (рис. 13.4):

– отправитель создает сообщение M;

– с помощью алгоритма хеширования SHA-1 создается 160-битовй хеш-код этого сообщения H(M);

– полученный хеш-код шифруется закрытым ключом отправителя D_A, в результате чего создается электронно-цифровая подпись (ЭЦП) отправителя - $D_A[H(M)]$. ЭЦП добавляется в начало сообщения (M);

– получатель использует открытый ключ отправителя E_A , чтобы дешифровать хеш-код: $H(M) = E_A[D_A[H(M)]]$;

– получатель генерирует новый хеш-код полученного сообщения M (т.е. H'(M)) и сравнивает его с дешифрованным хеш-кодом. Если хеш-коды H и H' совпадают, сообщение считается подлинным.

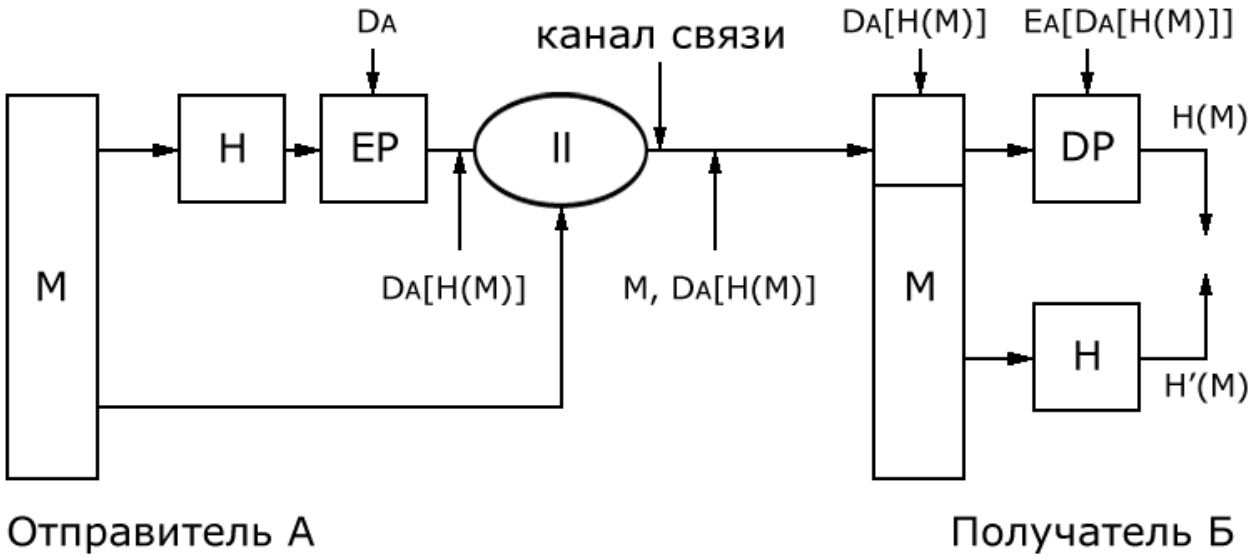


Рис. 13.4. Схема аутентификации сообщения

Ввиду того, что закрытый ключ отправителя имеется только у него, пользователь уверен в том, что данную подпись мог создать только владелец соответствующего секретного ключа. Надежность алгоритма хеширования SHA-1 дает получателю уверенность также в целостности данных, т.е. в том, что никто другой не мог создать другое сообщение с тем же хеш-кодом и, следовательно, с подписью их оригинального сообщения. Таким образом, схема рис. 13.4 обеспечивает уверенность в подлинности источника сообщений и целостность данных сообщений (т.е. аутентификацию сообщения).

Примечание. Как отмечено в приложении В, криптография с открытым ключом имеет

недостаток в низкой скорости, а поэтому применяется при шифровании/дешифровании коротких сообщений (ключа симметричного шифрования, хеш-кода). В приведенном примере (глава 2, раздел 2.5) канальное шифрование всего пакета сетевого уровня сети X.25 симметричной криптографией может быть заменено шифрованием короткого заголовка этого пакета с помощью асимметричной криптографии.

13.2.2. Протокол сетевого уровня IPSec

Настоящий раздел посвящен алгоритму протокола IPSec, механизмы реализации которого расположены ниже транспортного уровня эталонной модели TCP/IP на сетевом уровне (глава 12, рис. 12.1). Главным достоинством протокола IPSec, позволяющего поддерживать самые разнообразные приложения, является возможность шифрования и аутентификации всего потока данных на уровне IP. Защита может быть обеспечена любому приложению, т.е. протокол IPSec является прозрачным средством защиты для прикладных программ.

Механизмы защиты на уровне IP по протоколу IPSec обеспечивают ИБ не только сетевых приложений, имеющих свои встроенные средства, но и приложений, не обладающих такими возможностями.

Протокол IPSec обеспечивает защиту обмена данными в различных компьютерных сетях: локальных, корпоративных и открытых глобальных сетях типа Интернет. Приведем два примера применения IPSec, для которых в настоящем разделе дается описание использования этого протокола безопасности.

Защищенный доступ к филиалу организации или

к сети другой организации через Интернет

Протокол IPSec позволяет объединить в единую защищенную сеть компьютеры центрального офиса и его филиалов. Такая сеть, связанная с помощью общедоступной сети Internet, является виртуальной частной сетью VPN (Virtual Private Network).

Усиление защиты протоколов ИБ прикладного уровня

Защищенный канал, реализованный на прикладном уровне, защищает только определенную службу (файловую, гипертекстовую, почтовую и др.). При этом для каждого прикладного протокола необходимо разрабатывать собственные средства защиты. Использование IPSec усиливает защиту механизмов обеспечения ИБ, встроенных в протоколы прикладного уровня

(такие, как протоколы электронной коммерции и другие).

На рис. 13.5 показан пример использования IPSec. Здесь приведена корпоративная сеть из двух локальных вычислительных сетей, находящихся в разных местах. Под полезным грузом здесь понимается поле данных, в которое входят заголовки и информация уровней выше сетевого (т.е. транспортного и прикладного). Поле заголовка IPSec предназначено для аутентификации и конфиденциальности информации полезного груза. В рамках локальных сетей трафик IP корпоративной сети не защищается. Локальные вычислительные сети подключены через маршрутизаторы к сети Интернет, через которую обмениваются IP-текстами абоненты этих локальных сетей. Протокол IPSec обеспечивает ИБ этих пакетов. Эти протоколы установлены в маршрутизаторы по периметру сети. В маршрутизаторах производится шифрование потока данных, отправляемых в Интернет, и расшифрование данных, приходящих из Интернет. Все выполняемые при этом операции не заметны для рабочих станций и серверов локальных сетей.

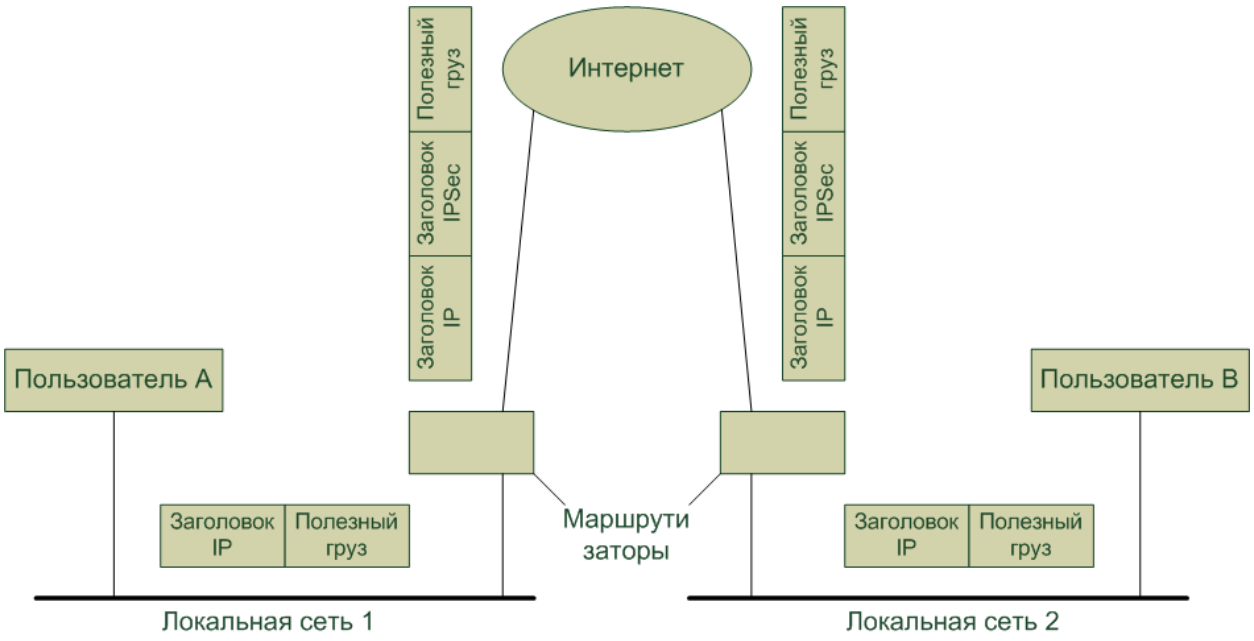


Рис. 13.5. Пример использования IPSec

13.2.2.1. Заголовки IPSec

В настоящем разделе приводится описание процедуры IPSec по аутентификации и конфиденциальности передаваемых сообщений.

На рис. 13.5 показано расширение заголовка IP – поле заголовка IPSec, которое позволяет реализовать протоколы AH и ESP.

Протокол AH обеспечивает только аутентификацию. Естественно, подобная защита данных

во многих случаях оказывается недостаточной. Принимающая сторона в этом случае получает лишь возможность проверить, что данные были отправлены именно тем узлом, от которого они ожидаются и дошли в том виде, в котором были отправлены. Однако от несанкционированного просмотра данных на пути их следования по сети протокол АН защитить не может, так как не шифрует их. Для шифрования данных необходим протокол ESP.

Протокол АН

Протокол «Заголовок аутентификации» АН, как было отмечено выше, обеспечивает аутентификацию сообщений. Формат заголовка АН в транспортном режиме показан на рис. 13.6. Под полезной нагрузкой здесь показано поле данных прикладного уровня.

Рис. 13.6. Заголовок аутентификации АН в транспортном режиме

Заголовок АН расположен между заголовком IP и заголовком TCP. Рассмотрим заголовок АН. Поле «Следующий заголовок» указывает код протокола, которым может быть протокол транспортного уровня (TCP или UDP) или протокол ESP, если он используется в комбинации с АН. Поле «Длина полезной нагрузки» указывает на длину заголовка АН. Поле «Индекс параметров защиты SPI» – это идентификатор соединения. Он вставляется отправителем и ссылается на конкретную запись в базе данных получателя. В этой записи содержится общий ключ и другая информация данного соединения. Поле «Порядковый номер» используется механизмом окна защиты от угрозы «повтор». В этом поле размещаются номера всех текстов, посылаемых по защищенной связи. Все пакеты получают универсальные номера, даже если они посылаются повторно. Имеется в виду, что повторно передаваемый пакет имеет номер, отличный от номера оригинального пакета (даже если порядковый номер TCP тот же самый). Это поле служит для предотвращения взлома путем повторной передачи. Порядковые номера никогда не повторяются. Если же окажутся использованными все 2^{32} номера, для продолжения общения устанавливается новая защищённая связь. Поле «Данные аутентификации» содержит код аутентификации сообщения по алгоритму HMAC (см. приложение Г, раздел Г.3). Спецификация протокола IPSec требует, чтобы любая реализация поддерживала две схемы алгоритма HMAC – с использованием хеш-кода MD5 и хеш-кода SHA-1. В обоих случаях вычисляется полное значение HMAC, равное длине хеш-кода (для MD5 128 бит и для SHA-1 160 бит), но затем оно усекается до 96 бит, что соответствует длине поля данных аутентификации, установленной по умолчанию.

Для вычисления HMAC берется информация заголовка IP-пакета, а также данные протокола следующего выше уровня (например, сегмент TCP или внутренний IP-пакет в туннельном режиме), которые не изменяются в пути следования. Примерами неизменяемых полей являются адреса отправителя и получателя IP-пакета, что защищает их от подмены злоумышленником. Поле «Время жизни» заголовка IP-пакета меняется при каждой пересылке через маршрутизатор.

Протокол ESP

Протокол «Защищенный полезный груз» ESP обеспечивает конфиденциальность. В качестве дополнительной возможности ESP может обеспечивать также аутентификацию. На рис. 13.7, а) показана область действия шифрования и аутентификации ESP в транспортном режиме, а на рис. 13.7, б) - в режиме туннелирования. Спецификации на IPSec требуют, чтобы протокол ESP поддерживал использование алгоритмов шифрования: DES, тройной DEA, IDEA и другие.

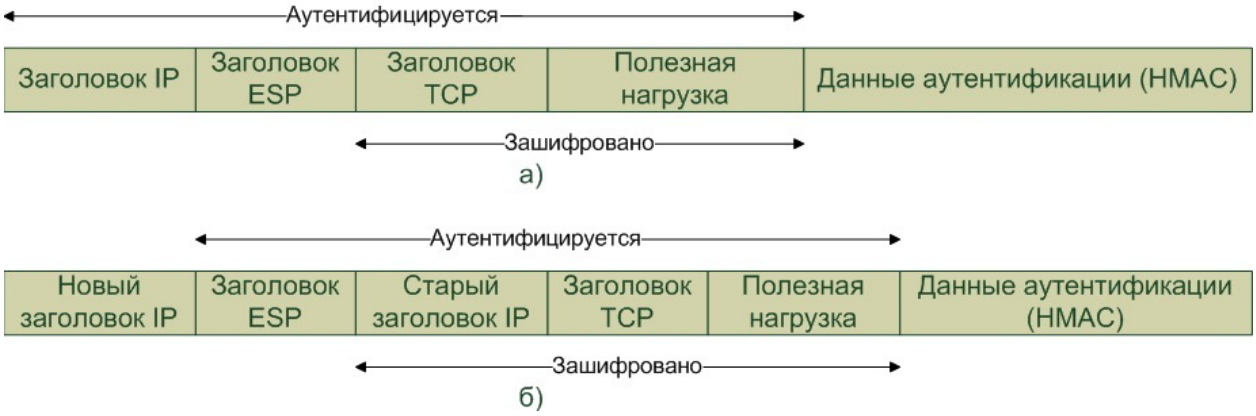


Рис. 13.7. Область действия шифрования и аутентификации ESP:

а) в транспортном режиме,

б) в режиме туннелирования

Заголовок ESP состоит из двух 32-разрядных полей «Индекс параметров защиты» SPI и «Порядкового номера», как и в заголовке AH.

ESP в транспортном режиме шифрование (и, как опция, аутентификация) осуществляет непосредственно между двумя оконечными компьютерами пользователей (рис.13.7, а). ESP, как и AH, обеспечивает проверку целостности при помощи HMAC, однако вместо того, чтобы включать хеш в заголовок, его вставляют после поля полезной нагрузки. Это видно на рис. 13.7, а). Такое расположение полей дает преимущество при аппаратной реализации метода. Оно заключается в том, что HMAC может подсчитываться во время передачи битов полезной нагрузки по сети и добавляться к ним в конец. Именно поэтому в Ethernet и других стандартах локальных сетей циклический код вставляется в концевик, а не в заголовок. При применении заголовка AH пакет приходится буферизовать и вычислять подпись, только после этого его можно отправлять. Это потенциально приводит к уменьшению числа пакетов, которые можно передать за единицу времени.

В транспортном режиме выполняются следующие операции.

- В узле источника блок данных, состоящий из концевика ESP и всего сегмента транспортного уровня, шифруется, и открытый текст этого блока заменяется шифрованным текстом, в результате чего формируется пакет IP для пересылки. Если выбрана опция аутентификации, то добавляется поле аутентификации.
- Пакет направляется адресату. Каждый промежуточный маршрутизатор должен

проверить и обработать заголовок IP. Шифрованный текст при этом остается неизменным.

– Узел адресата проверяет и обрабатывает незашифрованный заголовок IP-пакета. Затем на основе информации индекса параметров защиты в заголовке ESP дешифруются остальные части пакета, в результате чего становится доступным сегмент транспортного уровня в виде открытого текста.

Транспортный режим обеспечивает конфиденциальность для любого использующего этот режим приложения, что позволяет избежать необходимости реализации функций защиты в каждом отдельном приложении. Этот режим достаточно эффективен, а объем добавляемых к пакету IP данных при этом невелик. Недостатком этого режима является то, что IP-адреса пользователей являются открытыми и поэтому не исключается возможность анализа трафика пересылаемых пакетов. Например, если во время военного кризиса трафик между Пентагоном и Белым домом резко снижается и при этом так же резко растет трафик между Пентагоном и какой-нибудь военной базой в Колорадо, перехватчик может сделать из этого далеко идущие выводы.

Туннельный режим ESP в отношении возможности анализа трафика имеет преимущество перед транспортным режимом. Туннельный режим ESP предлагает шифрование всего пакета IP (рис. 13.7, б). В этом режиме заголовок ESP добавляется к пакету как префикс, а затем пакет вместе с концевиком ESP шифруются. Данный метод можно использовать, когда требуется исключить возможность проведения атак, построенных на анализе трафика.

Поскольку заголовок IP содержит адрес пункта назначения, нельзя просто передать шифрованный пакет IP с добавленным к нему в виде префикса заголовком ESP. Промежуточные маршрутизаторы не смогут обработать такой пакет. Таким образом, необходимо включить весь блок (заголовок ESP, шифрованный текст и данные аутентификации, если они есть) во внешний пакет IP с новым заголовком, который будет содержать достаточно информации для маршрутизации, но не для анализа трафика.

В то время как транспортный режим подходит для защиты соединений между узлами, поддерживающими ESP, туннельный режим оказывается полезным в конфигурации, предполагающей наличие шлюза защиты внутренней сети от внешних сетей. В туннельном режиме шифрование используют для обмена только между внешним узлом и шлюзом защиты или между двумя шлюзами защиты. Это разгружает узлы внутренней сети, избавляя их от необходимости шифрования данных, и упрощает процедуру распределения ключей, уменьшая число требуемых ключей. Кроме того, такой подход усложняет задачу анализа потока сообщений, направляемых конкретному адресату. Режим туннелирования еще более

усложняет анализ трафика, когда несколько TCP-соединений объединяются и обрабатываются в виде единого шифрованного потока. В этом случае злоумышленник не может проанализировать трафик, так как не знает, кто кому передает тексты и в каком количестве.

Рассмотрим случай, когда внешний узел (граничный маршрутизатор) соединяется с узлом внутренней сети, защищенной шлюзом и ESP, используется внешним узлом и шлюзом защиты. Тогда при пересылке сегмента транспортного уровня от внешнего узла к узлу внутренней сети выполняются следующие действия.

- Источник готовит внутренний пакет IP с указанием адреса пункта назначения, являющегося узлом внутренней сети. К этому пакету в виде префикса добавляется заголовок ESP. Затем пакет шифруется и к нему могут быть добавлены данные аутентификации. Полученный блок заключается во внешний пакет IP с новым заголовком IP, в котором адресом пункта назначения является адрес шлюза защиты.
- Внешний пакет отправляется шлюзу защиты сети пункта назначения. Каждый промежуточный маршрутизатор должен проверить и обработать внешний заголовок IP и все внешние заголовки расширений IP, оставляя при этом шифрованный текст неизменным.
- Шлюз защиты, получив пакет, проверяет и обрабатывает внешний заголовок IP. Затем на основе информации, предоставляемой индексом параметров защиты в заголовке ESP, шлюз защиты расшифровывает остальные части пакета, в результате чего становится доступным внутренний пакет IP в виде открытого текста. Этот пакет потом передается по внутренней сети.
- Внутренний пакет передается маршрутизатору внутренней сети или непосредственно узлу-адресату.

13.2.2.2. Транспортный и туннельный режимы

Заголовки AH и ESP поддерживают два режима использования: транспортный и туннельный. Суть этих двух режимов лучше всего понять в контексте описаний заголовков AH и ESP, о которых пойдет речь позже. Здесь же ограничимся кратким определением этих режимов.

Транспортный режим

Транспортный режим обеспечивает защиту для протоколов верхних уровней. Это значит, что защита транспортного режима распространяется на полезный груз пакета IP. Примерами могут быть сегменты TCP или UDP, размещающиеся в стеке протоколов хоста непосредственно над IP. Транспортный режим обеспечивает сквозную связь двух узлов (например, клиента и сервера).
ESP в транспортном режиме шифрует и, если нужно, аутентифицирует полезный груз IP, но не заголовок IP. AH в транспортном режиме предполагает аутентификацию полезного груза IP и некоторых частей заголовка IP.

Туннельный режим

Туннельный режим обеспечивает защиту всего пакета IP. Чтобы выполнить эту задачу, после добавления к пакету IP полей AH или ESP весь пакет вместе с полями защиты рассматривается как полезный груз некоторого нового «внешнего» пакета IP с новым внешним заголовком IP. Весь исходный (внутренний) пакет при этом пересылается через «туннель» от одной точки сети IP к другой, и ни один из маршрутизаторов на пути не может проверить внутренний заголовок IP. Поскольку пакет инкапсулирован в новый, больший пакет, этот новый пакет может иметь совершенно другие параметры источника и адресата, что, очевидно, усиливает защиту. Туннельный режим используется тогда, когда один или оба конца защищенной связи являются шлюзами защиты, например граничными маршрутизаторами, использующими IPSec. При использовании туннельного режима системы, размещенные за пределами транспортной IP-сети, могут осуществлять защищенный обмен данными без применения IPSec. Незащищенные пакеты, генерируемые такими системами, передаются по туннелям, проложенным через внешние сети с помощью защищенных связей в туннельном режиме, устанавливаемых программным обеспечением IPSec маршрутизатора на границе локальной сети.

Рассмотрим пример использования туннельного режима IPSec. Узел А сети генерирует пакет IP с адресом узла назначения В другой сети. Этот пакет направляется от создавшего пакет узла к маршрутизатору на границе сети А. Этот маршрутизатор выясняет, нужно ли пакет защищать с помощью IPSec. Если направляющийся от А в В через IP-сеть пакет требует применения IPSec, маршрутизатор на границе с сетью А выполняет функции IPSec и инкапсулирует этот IP-пакет во внешний пакет IP. Адресом отправителя этого внешнего пакета будет данный граничный маршрутизатор, а адресом получателя – граничный маршрутизатор IP-сети и сети получателя В. Теперь пакет направляется этому граничному маршрутизатору, а промежуточные маршрутизаторы будут иметь дело только с внешним заголовком IP. В граничном маршрутизаторе сети узла В и IP-сети внешний заголовок IP удаляется, а внутренний пакет доставляется узлу В. ESP в туннельном режиме шифрует и, если нужно, аутентифицирует весь внутренний пакет IP, включая внутренний заголовок IP. АН в туннельном режиме аутентифицирует весь внутренний пакет IP и некоторые части внешнего заголовка IP. Таким образом, при туннельном режиме все задачи по обеспечению информационной безопасности ложатся на IP-сеть общего пользования.

13.2.2.3. Защищенные связи

Для передачи данных между двумя компьютерами в конечных точках протокол IPSec предусматривает предварительное выполнение следующих шагов (фаз) [28].

1. Каждый компьютер должен быть, прежде всего, аутентифицирован.
2. После успешного прохождения аутентификации выполняются функции управления ключами по созданию общего главного ключа (мастер-ключа).
3. Создается защищенный канал SA (Security Association). При этом отправитель и получатель должны договориться о применяемых протоколах шифрования, определить общие ключи, времена их действия, а также другие параметры. На этой фазе с помощью общего секретного ключа выполняется функция управления ключами по созданию нескольких общих секретных ключей. Для защищенной связи протоколу IPSec требуется четыре общих секретных ключа: пара ключей для протокола аутентификации HMAC и пара ключей для шифрования в заголовке ESP. Ниже приводится список параметров защищенной связи. Эти параметры сохраняются в базе данных обеих сторон. Защищенная связь создается процедурой управления ключами с помощью одного из Интернет-протоколов обмена ключами IKE (Internet Key Exchange). Протокол IKE опирается на протоколы ISACMP (Internet Security Association and Key Management Protocol – протокол управления

ассоциациями и ключами защиты в сети Интернет) и Oakley. Протокол Oakley представляет собой вариант обмена ключами, выполняемый по усовершенствованной схеме Диффи-Хеллмана. Подробная реализация в IKE приведена в работе [9]. В следующем разделе, посвященном другому протоколу (TLS) обеспечения ИБ (на транспортном уровне TCP/IP), приводится описание алгоритма установления защищенной связи. Алгоритмы установления защищенной связи в IP-сети отличаются для разных протоколов ИБ. Во многом это относится к функциям управления ключами, которые определяют и распределяют общие секретные ключи.

Защищённая связь однозначно определяется следующими тремя характеристиками, которые передаются по защищенному каналу.

1. Индекс параметров защиты, SPI (Security Parameters Index). Строка битов, присваиваемая данной защищенной связи и имеющая только локальное значение. Индекс параметров защиты передается в заголовках AH и ESP, чтобы принимающая система имела возможность выбрать защищенную связь, в рамках которой должен обрабатываться принимаемый пакет.
2. Адрес IP пункта назначения. В настоящее время допускаются только однонаправленные адреса – это адрес пункта назначения защищенной связи, который может представлять систему конечного пользователя или сетевой объект типа брандмауэра или маршрутизатора.
3. Идентификатор протокола защиты. Этот идентификатор указывает, является ли данная связь защищенной связью AH или это защищенная связь ESP. Ядро IPSec по передаче данных составляет два протокола:

- **AH** (Authentication Header – заголовок аутентификации), гарантирующий аутентификацию передаваемых сообщений, т.е. подлинность источника сообщений и целостность данных.
- **ESP** (Encapsulating Security Payload – защищенный полезный груз), шифрующий передаваемые данные, т.е. обеспечивает конфиденциальность данных. ESP, кроме этого, может выполнить функции протокола AH.

Параметры защищенной связи

Защищенная связь характеризуется следующими основными параметрами.

- Счетчик порядкового номера, 32-битовое значение, используемое при генерировании значений поля порядкового номера в заголовках AH или ESP.
- Окно защиты от угрозы повтора. Используется для выявления воспроизведенных пакетов среди прибывающих пакетов AH или ESP.

- Информация AH. Алгоритм аутентификации, ключи, параметры продолжительности жизни ключей и другие необходимые параметры, используемые в рамках AH.
- Продолжительность жизни данной защищенной связи.
- Информация ESP. Алгоритм шифрования и аутентификации, ключи, значения инициализации, параметры продолжительности жизни ключей и другие необходимые параметры, используемые в рамках ESP.
- Режим протокола IPSec. Туннельный или транспортный. Режимы описаны в этом разделе ниже.
- Максимальная единица передачи (Maximum Transmission Unit – MTU). Максимальная единица передачи (максимальный размер пакета, который может быть передан без фрагментации) для всех участков маршрута и переменные времени существования.

13.2.2.4. Виртуальная частная сеть VPN-IPSec

На рис. 13.8 приведен пример структуры двух виртуальных частных сетей, построенных с помощью протокола ESP в туннельном режиме.

- VPN A пользователей локальных сетей A1, A2, и A3;
- VPN B пользователей локальных сетей B1, B2, и B3.

В новом незашифрованном заголовке содержится адрес граничного маршрутизатора Интернета, соединенного с локальной сетью. Адрес пользователя расшифровывается в этом граничном маршрутизаторе.

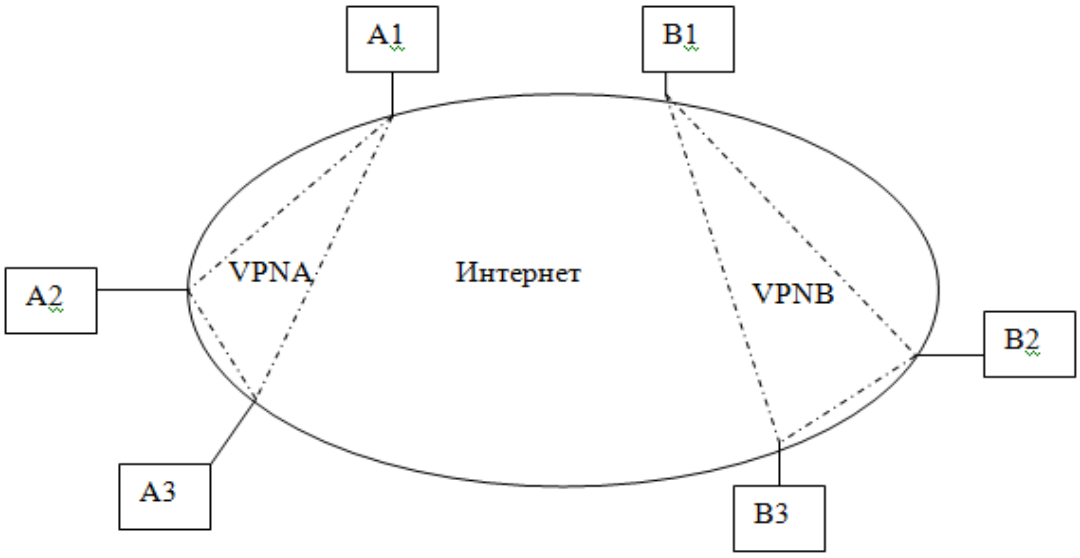


Рис.13.8. Пример структуры двух VPN на базе протокола IPSec

13.2.3. Протокол транспортного уровня TLS

Настоящее приложение посвящено протоколу обеспечения ИБ транспортного уровня TLS (Transport Layer Security), который применяется в сетях IP-телефонии протокола сигнализации SIP (см. глава 18), WiFi (см. глава 24) , WiMAX (см. глава 25). Протокол защиты транспортного уровня TLS стандартизирован в документе RFC 2246. Задача этого протокола обеспечить безопасную передачу данных с использованием протокола TCP. Этот механизм расположен в виде подуровня между транспортным и прикладным уровнями TCP/IP (см. главу 12). TLS является версией протокола защищенных сокетов SSL (Security Sockets Layer). Под сокетом понимается совокупность номера порта транспортного уровня и IP-адреса. Сокет однозначно идентифицирует прикладной процесс в Internet. Преимуществом использования протоколов ИБ на прикладном уровне является возможность оптимального построения механизма защиты в зависимости от требований конкретного приложения. Преимуществом протоколов SSL/TLS является обеспечение прозрачности средств защиты для прикладных программ.

TLS состоит из двух субпротоколов, один из которых предназначен для передачи данных по установленной защищенной связи (раздел 13.2.3.1), а второй для установления защищенной связи (раздел 13.2.3.2). Эта процедура установления защищённой связи SA (Security Association) является такой же ключевой, как и в IPSec (раздел 13.2.2.1). В отличие от приведенного выше описания SA протокола IPSec здесь более подробно приводится описание взаимной аутентификации, вычисление ключей, которые будут применяться для защиты данных и др.

13.2.3.1. Передача данных при использовании TLS

Одним из достоинств TLS является его полная программно-платформенная независимость. Протокол реализуется в виде многослойной среды. В качестве первого слоя используется транспортный протокол TCP. Вторым слоем, накладываемым на TCP, является TLS Record Protocol. Вместе эти два слоя, TCP и TLS Record Protocol, формируют ядро TLS.
На рис. 13.9 приведена схема передачи данных прикладного уровня по установленному защищенному соединению с обеспечением аутентификации сообщений (подлинности источника, целостности сообщений) и конфиденциальности их содержания.

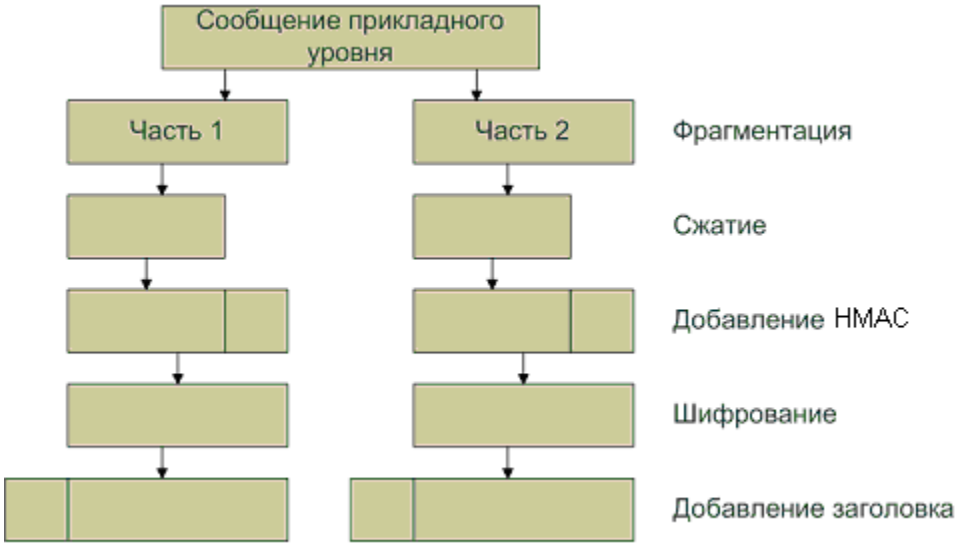


Рис. 13.9. Передача данных при использовании TLS

Сообщения, поступающие от браузера, фрагментируются на блоки длиной до 16 Кбайт. Если предусмотрено сжатие (процедура необязательная), каждый блок сжимается независимо. Затем к каждому блоку данных добавляется код аутентификации сообщений. В TLS для аутентификации сообщений используется стандартный протокол аутентификации сообщения HMAC, описание работы которого приводится в приложении Г, раздел Г3.
Следующим шагом, как видно из рис. 13.9, является шифрование блока данных вместе с добавленным к нему значением HMAC. Шифрование производится с помощью

криптографии с симметричным ключом.

Завершающим шагом в работе SSL/TLS является добавление заголовка, включающего:

- идентификатор протокола прикладного уровня, блоки данных которого передаются по TCP – соединению;
- длина сжатого фрагмента

и др.

13.2.3.2. Установление защищенной связи

На рис. 13.10 показана схема обмена сообщениями при установлении защищенной связи SA между клиентом и сервером. В сетях WiFi и WiMAX клиентом является беспроводный пользователь, а сервером аутентификации RADIUS-сервер. Процесс установления защищенной связи можно представить состоящим из следующих четырех этапов, составляющим протокол квитирования [9].

Этап 1. Определение характеристики защиты

На этом этапе производится инициализация соединения, и определяются связанные с ним характеристики защиты. Процесс инициализируется клиентом, который отправляет серверу сообщение «client hello» с параметрами: версия, случайные значения, идентификатор сеанса, комплект шифров, метод сжатия.

Приведём подробное описание двух из этих параметров – идентификатор сеанса и комплект шифров. Случайные значения используются для защиты от угрозы «повтор».

- Идентификатор сеанса.

Работа TLS описывается в двух важных понятиях – сеанс и соединение. Сеанс определяет набор параметров защиты, которые могут использоваться несколькими соединениями. Идентификатор сеанса говорит о намерении клиента создать новый сеанс или создать новое соединение в рамках того же сеанса.

- Комплект шифров.

Каждый комплект шифров определяет алгоритм обмена ключей и список, состоящий из следующих полей:

- алгоритм шифрования (RC4, тройной DEA, IDEA и др.);
- алгоритм хеш-функции (SHA-1, MD5);

- тип шифра (поточный, блочный);
- длина хеш-кода;
- длина вектора инициализации (IV) режима блочных кодов и др.

Протокол TLS поддерживает следующие методы обмена ключей для шифрования с общим ключом и для вычислений значений по протоколу HMAC. При этом могут быть использованы как протокол с открытым ключом (приложение В), так и протокол по методу Диффи-Хеллмана (приложение Д).

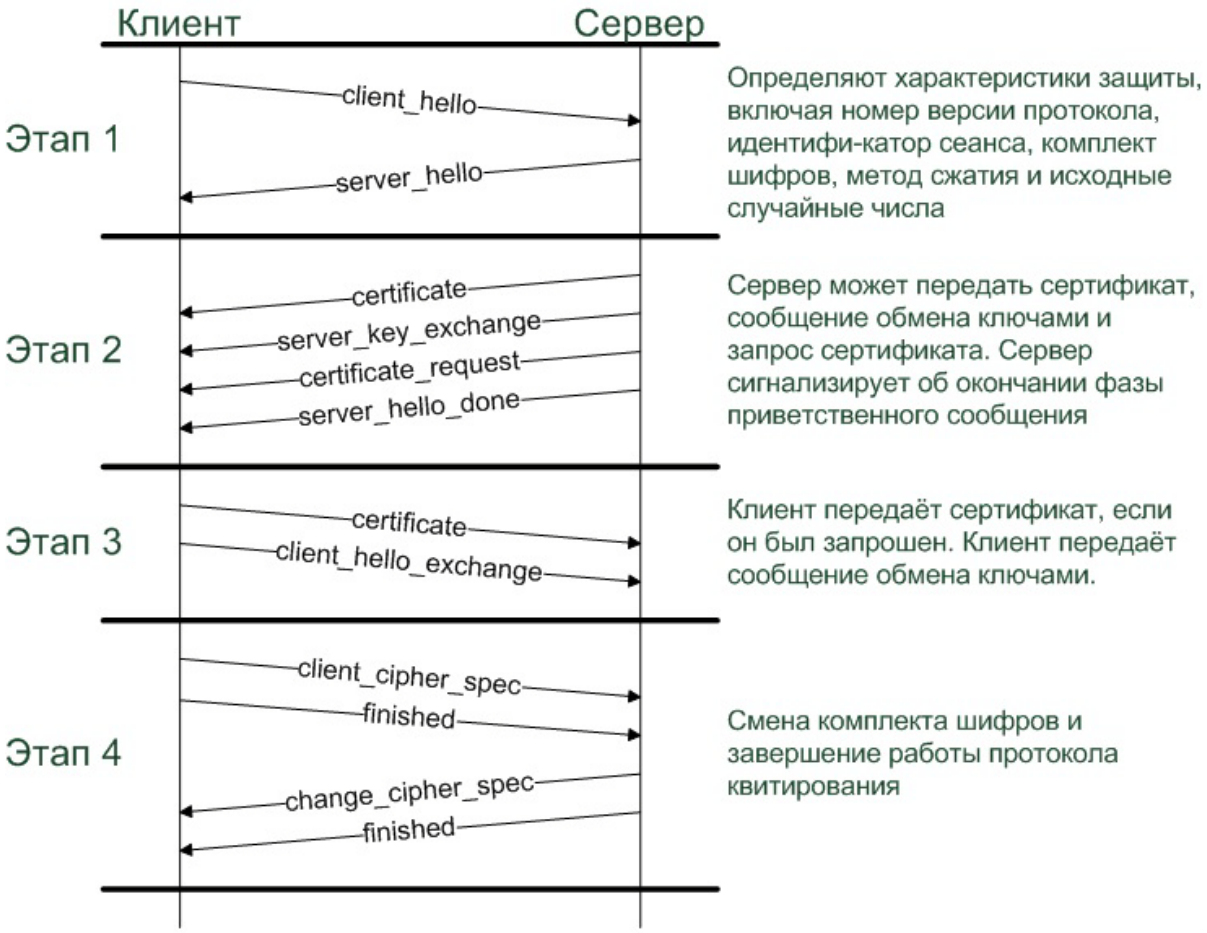


Рис. 13.10. Схема обмена сообщениями при установлении защищенного соединения

- RSA. Секретный ключ шифруется с помощью открытого ключа RSA получателя. Для этого отправителю должен быть доступен сертификат открытого ключа получателя и цепочка сертификатов для проверки достоверности этого ключа (приложение В). Более подробное изложение этого метода приводится в главе 17 (раздел 17.5) при изложении аутентификации и обмена ключами в сети ISDN.
- Метод Диффи-Хеллмана с фиксированными параметрами (Fixed Diffie-Hellman). Метод обмена ключами по схеме Диффи-Хеллмана, при котором сертификат сервера содержит открытые параметры алгоритма Диффи-Хеллмана, подписанные центром сертификации. Клиент сообщает свои параметры алгоритма Диффи-Хеллмана либо в сертификате, если требуется аутентификация клиента, либо в сообщении обмена ключами. Это обеспечивает защиту от угрозы «человек посередине» (приложение Д).
- Метод Диффи-Хеллмана с одноразовыми параметрами (Ephemeral Diffie-Hellman). Этот метод применяется для создания временных (одноразовых) секретных ключей. В этом случае стороны обмениваются открытыми ключами Диффи-Хеллмана, подписанными закрытым ключом RSA отправителя. Получатель для проверки подписи может использовать соответствующий открытый ключ. Для аутентификации открытых ключей применяются сертификаты. Это обеспечивает защиту от угрозы «человек посередине» (приложение Д).
- Анонимный метод Диффи-Хеллмана (Anonymous Diffie-Hellman). Предполагает использование базового алгоритма Диффи-Хеллмана, но аутентификация не выполняется. Иными словами, каждая из сторон отправляет свои открытые параметры для алгоритма Диффи-Хеллмана другой стороне без аутентификации. Данный подход оказывается уязвимым к атакам «человек-посередине», когда с обеими сторонами по анонимному методу Диффи-Хеллмана обмен ключами проводит злоумышленник.

После отправления сообщения «client hello» (приветствие клиента), клиент ожидает от сервера сообщения «server hello» (приветствие сервера), которое содержит согласованные алгоритмы шифра, алгоритмы обмена ключами и другие параметры, что и в сообщении «client hello».

Этап 2. Аутентификация и обмен ключами сервера

Данный этап начинается с отправки сервером его сертификата, если требуется аутентификация сервера. Отправляемое сообщение содержит сертификат X.509 или цепочку таких сертификатов. Сообщение certificate (сертификат) требуется для любого из предлагаемых методов обмена ключами, кроме анонимного метода Диффи-Хеллмана.

Обратите внимание на то, что при использовании метода Диффи-Хеллмана с фиксированными параметрами сообщение сертификата играет роль сообщения обмена ключами, поскольку в нем содержатся предлагаемые сервером открытые параметры алгоритма Диффи-Хеллмана.

Затем может быть отправлено сообщение «server_key_exchange» (обмен ключами сервера). Отправка такого сообщения не требуется в двух случаях: (1) когда сервер отправил сертификат для метода Диффи-Хеллмана с фиксированными параметрами, и (2) когда предлагается использовать схему обмена ключами RSA. Сообщение «server_key_exchange» необходимо тогда, когда используются следующие схемы.

- Анонимный метод Диффи-Хеллмана. Сообщение содержит два глобальных значения, необходимых для использования метода Диффи-Хеллмана (некоторое простое число и его первообразный корень), а также открытый ключ сервера для алгоритма Диффи-Хеллмана.
- Метод Диффи-Хеллмана с одноразовыми параметрами. Сообщение содержит такие же три параметра, как и в анонимном методе Диффи-Хеллмана, а кроме того, подпись для этих параметров.

Обычно подпись создается с помощью вычисления хеш-кода сообщения с последующим ее шифрованием закрытым ключом отправителя.

Функция хеширования вычисляется для аргумента, включающего не только параметры Диффи-Хеллмана или RSA, но и оба сообщения приветствия на этапе 1 (рис. 13.10). Это обеспечивает защиту от атак воспроизведения сообщений и атак фальсификации ответа.

После этого неанонимный сервер (т.е. сервер, не использующий анонимный метод Диффи-Хеллмана) может запросить сертификат клиента. Сообщение «certificate_request» (запрос сертификата) включает два параметра: «certificate_type» (тип сертификата) и «certificate_authorities» (центры сертификации). Тип сертификата указывает применяемый алгоритм шифрования с открытым ключом и может быть следующим.

- RSA, только для подписи.
- RSA для метода Диффи-Хеллмана с одноразовыми параметрами.

Вторым параметром сообщения «certificate_request» является список имен допустимых центров сертификации.

Последним (и единственным обязательным) сообщением второго этапа является сообщение «server_done», свидетельствующее о завершении фазы приветствия сервера. Это сообщение не имеет параметров. После отправки этого сообщения сервер переходит в режим ожидания ответа клиента.

Этап 3. Аутентификация и обмен ключами клиента

Получив сообщение «server_done», клиент должен убедиться в том, что сервер предоставил действительный сертификат (если это требуется), и что параметры сообщения «server_hello» являются приемлемыми. Если проверка завершается успешно, клиент отправляет серверу одно или несколько сообщений, речь о которых пойдет ниже.

Если сервер запросил сертификат, клиент начинает данный этап с отправки серверу сообщения «certificate».

Следующим идет сообщение «client_key_exchange» (обмен ключами клиента), которое для этого этапа является обязательным. Содержимое этого сообщения зависит от выбранного метода обмена ключами и может быть следующим:

- RSA. Клиент генерирует 48-байтовый *предварительный ключ* и шифрует его с помощью открытого ключа из сертификата сервера. Этот предварительный ключ позволяет вычислить *главный ключ*, как будет показано ниже.
- Метод Диффи-Хеллмана с одноразовыми параметрами, или анонимный метод Диффи-Хеллмана. Отправляются открытые параметры клиента для метода Диффи-Хеллмана.

Для метода Диффи-Хеллмана так же, как для RSA предусмотрено создание предварительного ключа у клиента и сервера. На основании предварительного ключа клиент и сервер по специальному алгоритму с использованием хеширования создают главный ключ. При этом используются случайные значения (нонсы, оказии) в сообщениях этапа 1 (рис. 13.10). Из главного ключа создается набор ключей различного назначения. Процедура их создания аналогична процедуре создания главного ключа из предварительного ключа. Приведем список этих ключей.

- Ключ симметричного шифрования, используемый сервером для шифрования данных и расшифрования их клиентом.
- Ключ симметричного шифрования, используемый клиентом для шифрования данных и расшифрования их сервером.
- Секретный ключ, применяемый клиентом для вычисления кода аутентичности, используемого по протоколу HMAC для аутентификации сообщений в части целостности данных и неотказуемости.
- Секретный ключ, применяемый сервером для вычисления кода аутентичности, используемого по протоколу HMAC для аутентификации сообщений в части

целостности данных и неотказуемости.

- Вектор инициализации IV, используемый в режиме блочного шифрования (Приложение Б, разд. Б.2.2.). . Используются два вектора инициализации – один при передаче сообщений клиентом, другой – сервером.

Этап 4. Завершение

Этот этап завершает создание защищенной связи SA. Клиент отправляет сообщение «change_cipher_spec» (изменение параметров шифрования), копирует параметры состояния ожидания в поле текущего состояния. В ответ клиент немедленно отправляет сообщение «finished», зашифрованное новым алгоритмом с новыми ключами и секретными значениями. Сообщение «finished» подтверждает, что процессы обмена ключами и аутентификация завершились успешно.

В ответ на эти два сообщения сервер посылает свое сообщение «change_cipher_spec», переводит параметры состояния ожидания в текущее состояние и посылает свое сообщение «finished». Теперь клиент и сервер могут начать обмен данными на уровне приложения.

13.2.4. Протоколы ИБ при маршрутизации

Протоколы маршрутизации RIP, OSPF и BGP уязвимы в отношении фальсификации сообщений между соседними маршрутизаторами. Злоумышленник может выдать себя за новый или существующий маршрутизатор. Рассылая нелегитимные RIP или OSPF-сообщения обновления маршрутизации, он может нарушить схему маршрутизации в сети или направить часть трафика в системе через свой компьютер, то есть получит возможность прослушивать, изменять или уничтожать передаваемые данные. К таким сообщениям, в частности, относятся нелегитимные сообщения обновления маршрутизации протоколов RIP и OSPF на втором уровне, а BGP- на третьем уровне TCP/IP. Реализация таких угроз информационной безопасности относится к атакам типа отказ в обслуживании (DoS - Denial of Service), которая выражается в нарушении выполнения определенных функций (в данном случае функции маршрутизации). В качестве одного из показателей риска угрозы ИБ является последствие после ее реализации и при отсутствии защиты. В случае атаки DoS с помощью нелегитимных сообщений обновления маршрутизации последствием является вывод из работы части IP-сети из-за нарушения функции маршрутизации. Защитой от таких атак служат механизмы аутентификации, некоторые алгоритмы которых приведены в приложениях В и Г. Протокол аутентификации (подлинность источника) сообщений в RIP и OSPF специфицирован стандартом RFC-2453 и определен с помощью обычного пароля,

который передаётся в открытом виде. Такая защита слабая, если злоумышленник имеет возможность прослушивать сеть.

Стандартом RFC-2082 [29] определён более сильный механизм защиты - аутентификация сообщений, предусматривающая проверку подлинности источника сообщений между соседними маршрутизаторами, а также целостность этих сообщений (т.е. подлинность их поступления от источника). Алгоритм такой аутентификации следующий. К сообщению обновления маршрутизации протоколов маршрутизации RIP, OSPF или BGP добавляется секретный ключ. Отправитель формирует хеш-функцию по стандартизированному протоколу MD5 такого объединенного с ключом сообщения. Хеш-функция является односторонней функцией и не позволяет восстановить исходное сообщение, включающее общий ключ соседних маршрутизаторов. Сообщение обновления маршрутизации вместе с полученной хеш-функцией пересылается получателю. Сам секретный ключ по сети не передается. Получатель проделывает ту же операцию: берёт полученное сообщение, добавляет к нему свою копию секретного ключа, вычисляет хеш-функцию и сравнивает результат с полученной хеш-функцией. Если она не совпадает, то сообщение отбрасывается.

ГЛАВА 14. Интегральное и дифференцированное качество обслуживания. Стандарты QoS в IP-сетях

14.1. Качество обслуживания

Сеть Интернет, кроме передачи данных, все больше и больше используется для поддержки мультимедийного трафика. В первую очередь это относится к передаче голоса поверх IP (VoIP), которая в отличие от передачи данных очень чувствительная к задержкам. При описании процедур работы сети ATM было показано, что различные виды информации мультимедийной сети требуют поддержки соответствующих механизмов обеспечения качества обслуживания QoS.Традиционные IP-сети не гарантируют никакого показателя QoS. Взять за основу сеть ATM, обеспечивающую передачу с необходимым QoS любого мультимедийного трафика, практически оказалось невозможным для сетей общего пользования из-за больших затрат. Это относится к каждому из вариантов: - построение сети ATM для трафика реального времени (речь, видео), требующую малую задержку (с сохранением IP-сети для передачи данных); - полная замена IP- сети на сеть ATM. Таким образом, возникла необходимость обеспечить поддержку различного мультимедийного трафика с разнообразными требованиями к уровню QoS в рамках архитектуры IP-сети. Механизмы QoS при рассмотрении их для использования в среде IP можно разделить на три категории: один подход оперирует в режиме сквозной передачи из «конца в конец» (end - to - end), другой функционирует на уровне транзитов (hop – by – hop) и третий совершенно игнорирует IP, используя новую технологию многопротокольной коммутации по меткам MPLS. Первая категория определяет архитектуру интегрального обслуживания IntServ, а вторая – дифференцированного обслуживания DiffServ (DS) [30].

14.2. Интегральное обслуживание IntServ

Главный протокол архитектуры интегрального обслуживания, разработанный IETF, называется протоколом резервирования ресурсов RSVP (Resource reservation Protocol). Как следует из названия, протокол предназначен для резервирования ресурсов. RSVP является протоколом сигнализации, который позволяет приложениям информировать сеть о своих требованиях. На основе этих требований сеть может либо резервировать внутри себя ресурсы, чтобы гарантировать выполнение требований, либо отказать приложению. Протокол

RSVP позволяет запрашивать, например, гарантированный показатель трафика, задержку, максимальный уровень потерь блоков данных. Рассмотрим процедуру резервирования по протоколу RSVP (рис. 14.1).

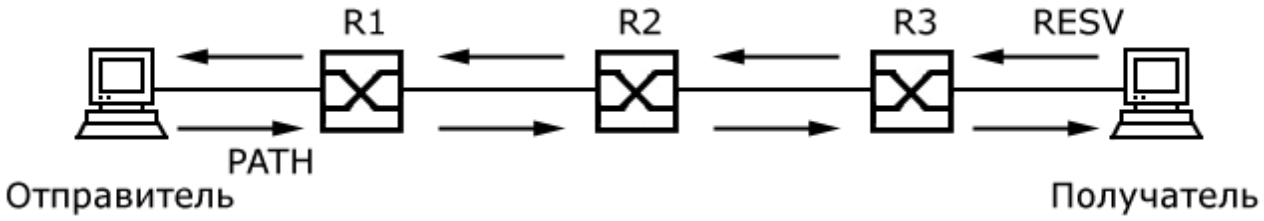


Рис. 14.1. Резервирование ресурсов с помощью RSVP
R1, R2, R3 – маршрутизаторы.

Как показано на рисунке 14.1, протокол RSVP передает информацию с использованием двух типов сообщений: PATH и RESV. Сообщения PATH передаются от отправителя к одному или нескольким получателям и включают в себя:

- спецификацию потока данных Tspec, которая определяет тип потока данных приложения, входящего в сеть (T означает трафик);
- шаблон отправителя (IP-адрес, UDP/TCP порт как опция).

Получив сообщение PATH, получатель передает отправителю сообщение RESV, идентифицируя сеанс, для которого производится резервирование, а также спецификацию Rspec (R означает резервирование, Reserve). Rspec включает уровень QoS, требуемый получателем. После того как резервирование выполнено, маршрутизаторы, находящиеся на маршруте, могут идентифицировать пакеты, принадлежащие к определенному блоку зарезервированных ресурсов, путем анализа следующих полей в заголовке протокола IP и в заголовке транспортного протокола: IP-адрес получателя, порт получателя, IP-адрес отправителя и его порт. Пакеты, идентифицированные таким образом, называются зарезервированным потоком. К пакетам в зарезервированном потоке применяются определенные правила для того чтобы не генерировался больший трафик, чем объявлено в спецификации Tspec. Для пакетов потока также устанавливается соответствующий приоритет обработки с целью обеспечения требуемого уровня обслуживания.

При разработке протокола RSVP предусматривалось резервирование ресурсов для индивидуальных микропотоков приложений. Однако такой подход имеет несколько

практических недостатков. При его использовании каждый элемент сети на всем пути следования пакета, включая оконечные системы, должен иметь полную информацию протокола RSVP и участвовать в сигнализации, требуемой механизмом QoS. На каждом сетевом элементе, лежащем на маршруте, должна поддерживаться информация каждого резервирования. Такое требование может привести к потенциальному расширению сети до состояния, когда через базовую IP-сеть будут проходить сотни тысяч потоков. При этом требуется предварительная договоренность при установке канала для каждого потока. Это не позволяет расширить систему в достаточной мере. Поэтому в системах с тысячами потоков интегральное обслуживание применить не удастся. В результате выжило очень мало реализаций RSVP в IP-сетях. Однако этот протокол может выполнить резервирование для объединенных потоков данных. Это позволило использовать протокол RSVP в технологии MPLS.

14.3. Дифференцированное обслуживание DiffServ

По причине указанных выше недостатков модели IntServ комитетом IETF был создан упрощённый подход к обеспечению качества обслуживания в IP-сетях - модель дифференцированного обслуживания DiffServ. При такой модели не требуется предварительной настройки включения в процесс всех устройств вдоль маршрута. Реализация DiffServ осуществляется локально в каждом маршрутизаторе сети.

14.3.1. Модель DiffServ

Модель DiffServ ориентирована на разделении всего трафика на небольшое число классов и на выделение сетевых ресурсов отдельно для каждого такого класса, а не для каждого информационного потока, как это предусмотрено в модели IntServ. Класс маркируется непосредственно в поле кода дифференцированного обслуживания DSCP (DiffServ Code Point) пакета. Поле DSCP занимает 6 бит байта ToS (Type of Service) заголовка IP-пакета. Поле DSCP определяет механизм обработки различных информационных потоков PHB (Per-Hop Behavior), который выражает порядок обработки пакета в узле в отношении приоритета очерёдности обработки и отбрасывания пакета при перегрузке. IETF определил набор из 14 классов обслуживания трафика. В их число входит класс негарантированного обслуживания BE (Best Effort), при котором трафик не получает никакой гарантии и класс срочной пересылки пакетов EF (Expedited Forwarding), при котором трафик получает минимальную задержку и низкую вероятность потерь (для речи и видео). Остальные 12

классов обслуживания определены документом RFC 2597 и относятся к гарантированной пересылке AF (Assured Forwarding). Четыре класса позволяют выделить четыре профиля трафика в соответствии с требованиями пользователя.

Внутри каждого класса пакеты маркируются пользователем или поставщиком услуг с помощью одного из трёх значений старшинства сброса пакетов. В случае перегрузки старшинство отмены пакетов определяет относительную значимость пакета внутри класса гарантированной пересылки. Домен DS состоит из множества маршрутизаторов. Маршрутизаторы в домене DiffServ представляют собой внутренние и граничные узлы. Внутренние узлы реализуют простой механизм обработки пакетов PHB (Per-Hop Behavior) на основе своих кодовых значений DSCP.

Сюда включается дисциплина очереди для предпочтительной обработки в зависимости от DSCP и правила отмены передачи пакетов, определение какие пакеты необходимо отбросить первыми в случае перегрузки. Пограничные узлы включают не только механизмы PHB, но также и более сложные механизмы регулирования трафика. В первую очередь это относится к разделению пакетов на различные классы (на основе DSCP либо на основе полей заголовка пакета, либо на основе полезной нагрузки пакета). После того как поток классифицирован, в пограничном узле производится оценка его потребности в ресурсах по результатам измерений представленного трафика на соответствие профиля. В случае несоответствия в пограничном узле могут быть использованы следующие механизмы регулирования трафика:

- задержка пакетов при превышении скорости трафика, определённой в профиле этого класса;
- повторная маркировка пакетов другими кодовыми значениями при превышении требований профиля;
- отмена передачи пакетов, когда скорость пакетов данного класса превышает скорость трафика, заданную в профиле.

Основное преимущество DiffServ заключается в том, что это простой метод классификации различных прикладных сервисов и позволяет обеспечить некоторое приближение к выполнению требований пользователей к качеству обслуживания. Механизм DiffServ использован в технологии MPLS.

14.3.2. Структурная схема программного обеспечения обработки очередей в модели DiffServ

Отметим, что для класса BE значение DSCP=000000, EF – 1011110. Для класса AF значение DSCP равно xyzabo, где xyz – приоритет обслуживания, а ab – биты приоритета сброса при перегрузке. Значения приоритета обслуживания следующие – xyz=001 (класс 1), 010 (класс 2), 011 (класс 3), 100 (класс 4). Наивысший приоритет обслуживания 4. Приоритет сброса 3 наибольший, что означает сброс пакета при перегрузке раньше, чем пакета приоритета сброса 2 или 1. На рис. 14.2 приведена в качестве примера структурная схема фоновой программы внутреннего маршрутизатора по обработке очередей пакетов классов AF на передачу в модели DiffServ.

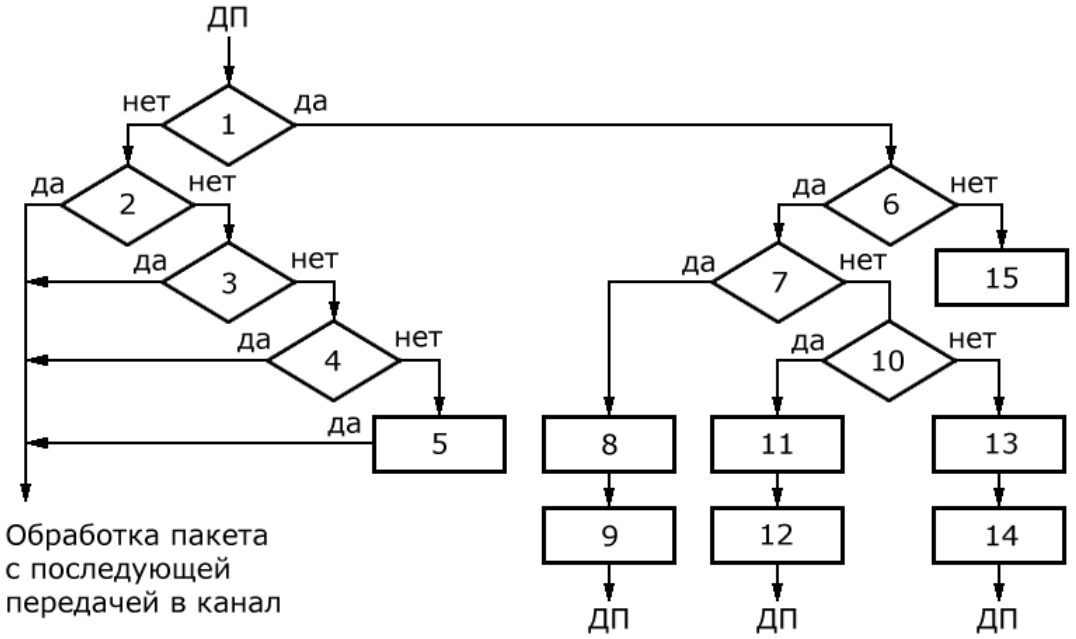


Рис. 14.2. Структурная схема фоновой программы маршрутизатора по обработке очередей пакетов на передачу в модели DS

Пакет относится к гарантированной пересылке, при которой программное обеспечение обрабатывает следующие 16 очередей обслуживания: 0_1,0_2,0_3,0_4 – очереди пакетов приоритетов обслуживания 1,2,3,4; 0_{11},0_{12},0_{13}, – очереди приоритетов 1,2,3 сброса пакетов приоритета обслуживания 1; 0_{21},0_{22},0_{23}, – очереди приоритетов 1,2,3 сброса пакетов приоритета обслуживания 2; 0_{31},0_{32},0_{33}, – очереди приоритетов 1,2,3 сброса пакетов приоритета обслуживания 3; 0_{41},0_{42},0_{43}, – очереди приоритетов 1,2,3 сброса пакетов приоритета обслуживания 4. Очереди пакетов приоритетов обслуживания состоят из списков, в поле 3 которых находятся сами пакеты (рис. 14.3, а). Очереди приоритетов сброса состоят из списков, в поле 3 (рис. 14.3, б) которых находятся адреса

пакетов, стоящих в соответствующих очередях пакетов приоритета обслуживания (рис. 14.3, а). Поля 1 и 2 в обоих случаях являются адресами связки в очередях. Это позволяет составить программное обеспечение с меньшим числом команд, что является одной из наиболее важных задач для обеспечения большего числа обслуживаемых пользователей коммутационной станцией и лучших показателей качества обслуживания.

1	2	3
Адрес предыдущей строки в очереди приоритета обслуживания	Адрес следующей строки в очереди приоритета обслуживания	Пакет

а)

1	2	3
Адрес предыдущей строки в очереди приоритета сброса пакетов	Адрес следующей строки в очереди приоритета сброса пакетов	Адрес пакета в очереди пакетов приоритета обслуживания

б)

Рис. 14.3. Формат элемента в очереди пакетов приоритета обслуживания (а) и в очереди приоритетов сброса пакетов (б)

Использование списка очередей в программном обеспечении модели DS

С целью упрощения описания работы схемы программного обеспечения на рис. 14.2 принято условие нахождения только одного пакета в одной из очередей приоритетов обработки пакетов. Будем считать, что наивысший приоритет обслуживания 4 относится к очереди службы «речь» по причине критичности к задержке, а приоритет обслуживания 1 к службе «передача данных». Поэтому в приведенном ниже примере структурной схемы программного обеспечения в первую очередь обработке при отсутствии перегрузки подлежат пакеты очереди приоритета обслуживания 4, а при перегрузке в первую очередь подлежат сбросу пакеты приоритета сброса 3 этой же очереди приоритета обслуживания 4. Под обслуживанием понимается передача пакета на дальнейшую обработку с последующей передачей в канал связи. Под сбросом понимается установка блока в очередь свободных блоков Освоб.

Операция 1. Режим перегрузки? Если нет, то переход к операции 2. Иначе переход к операции 6.

Операция 2. Есть пакеты в очереди приоритета обслуживания 4 [$N(O_4)\neq 0$]? Если да, то передача этого пакета для обработки с последующей передачей его в канал. Иначе переход к операции 3.

Операция 3. Есть пакеты в очереди приоритета обслуживания 3 [$N(O_3)\neq 0$]? Если да, то передача этого пакета для обработки с последующей передачей его в канал. Иначе переход к операции 4.

Операция 4.Есть пакеты в очереди приоритета обслуживания 2 [$N(O_2)\neq 0$]? Если да, то передача этого пакета для обработки с последующей передачей его в канал. Иначе переход к операции 5.

Операция 5. Передача пакета в очереди приоритета обслуживания $I(O_1)$ для обработки с последующей передачей его в канал.

Операция 6. Есть пакеты в очереди приоритета обслуживания 4 [$N(O_4)\neq 0$]? Если да, то переход к операции 7. Иначе переход к операции 15.

Операция 7. Есть пакет приоритета обслуживания 4 приоритета сброса 3 [$N(O_{43})\neq 0$]? Если да, то переход к операции 8. Иначе переход к операции 10.

Операция 8. По содержимому в поле 3 адреса первого блока адресов в O_{43} определить адрес пакета O_4, подлежащий сбросу. Снять первый блок в O_{43} и поставить в очередь свободных блоков Освоб.

Операция 9. Снять пакет в O_4 с адресом, определенным в операции 8, и поставить его в очередь свободных $O_{своб}$.

Операция 10. Есть пакет приоритета обслуживания 4 приоритета сброса 2 [$N(O_{42})\neq 0$]? Если да, то переход к операции 11. Иначе переход к операции 13.

Операция 11. По содержимому в поле 3 адреса первого блока адресов в O_{42} определить адрес пакета в O_4, подлежащий сбросу. Снять первый блок в O_{42} и поставить в очередь свободных $O_{своб}$.

Операция 12. Снять пакет в O_4 с адресом, определенным в операции 11, и поставить его в $O_{своб}$.

Операция 13. По содержимому в поле 3 адреса первого блока адресов в O_{41} определить адрес пакета в O_4, подлежащий сбросу. Снять первый блок в O_{41} и поставить в очередь свободных $O_{своб}$.

Операция 14. Снять пакет в O_4 с адресом, определенным в операции 13, и поставить его в $O_{своб}$.

Операция 15 и далее аналогичны операциям 7-14, но вместо очередей O_4, O_{43}, O_{42}, O_{41} анализируются очереди O_3, O_{33}, O_{32}, O_{31}; O_2, O_{23}, O_{22}, O_{21}; O_1, O_{13}, O_{12}, O_{11}.

14.4. Стандарты по качеству обслуживания в IP-сетях

Одним из важнейших направлений перспективных сетей связи, является пакетно-коммутируемая сеть на базе протокола IP, позволяющей передавать как голос, так и данные. Одной из задач этой конвергенции является обеспечение качества обслуживания QoS, поскольку современные IP-сети не гарантируют никакого качества. Для того чтобы реализовать конвергенцию IP-сетей и сетей ТфОП, IP-сети должны обеспечить качество обслуживания из «конца в конец». В рамках работ ITU-T по стандартизации качества обслуживания предполагаются следующие этапы решения задачи обеспечения QoS для конвергированных сетей ТфОП/IP с учетом перехода к сетям нового поколения NGN (New Generation Network):

- создание согласованного общего набора рабочих характеристик сетей IP и норм для этого набора характеристик;
- внедрение сетевых механизмов, которые будут обеспечивать заданные показатели качества обслуживания в конфигурации «терминал - терминал»;

- вложение нормированных показателей качества обслуживания в протоколы сигнализации;
- разработка архитектуры сетевых механизмов поддержки.

В 2002г. 13-я Исследовательская Комиссия ITU-T опубликовала два международных стандарта, которые отвечают первому из перечисленных этапов. Рекомендация ITU-T Y.1540 описывает стандартные сетевые характеристики для передачи пакетов в сетях IP. Рекомендация ITU-T Y.I541 определяет нормы для параметров, определённых в рекомендации Y.1540, между двумя граничными сетевыми интерфейс - точками подключения оконечных терминальных устройств.

Эти рекомендации важны для операторов и провайдеров, производителей оборудования и конечных пользователей. Сетевые провайдеры будут использовать данные рекомендации при планировании, развёртывании и оценке сетей IP в соответствии с требованиями конечных пользователей к качеству обслуживания. Производители будут опираться на эти рекомендации при создании оборудования, которое должно отвечать спецификациям сетевых провайдеров. Наконец, конечные пользователи (в первую очередь корпоративные) смогут применить рекомендации Y.1540 и Y.1541 при оценке характеристик реально функционирующих IP-сетей с позиций соответствия этих характеристик требованиям потребителей. Рассмотрим некоторые детали рекомендаций Y.1540 и Y.1541, касающиеся основных сетевых характеристик качества обслуживания QoS в IP-сетях.

14.4.1. Рекомендация ITU-T Y.1540

Следующие пять сетевых характеристик рассматриваются в рекомендации ITU-T Y.1540 как наиболее важные по степени их влияния на сквозное качество обслуживание (от источника до получателя), оцениваемое пользователем на субъективной основе:

- производительность сети;
- надёжность сети/сетевых элементов;
- задержка;
- вариация задержки (джиттер);
- потери пакетов.

Производительность сети

Производительность сети, или скорость передачи данных пользователя, определяется как

эффективная скорость передачи, измеряемая в бит/с. Следует иметь в виду, что значение этого параметра не совпадает с максимальной пропускной способностью сети. В рекомендации ITU-T Y.1540 не приведены нормативные характеристики производительности сети, которые отличаются для различных приложений. Вместе с тем в рекомендации ITU-T Y.I541 отмечено, что параметры, связанные с эффективной скоростью передачи, могут быть определены методом, описанным в рекомендации ITU-T Y.1221.

Надёжность сети/сетевых элементов

Пользователи обычно ожидают высокого уровня надёжности от систем связи. Надёжность сети может быть определена через ряд параметров, из которых наиболее часто используется коэффициент готовности, вычисляемый как отношение времени простоя объекта к суммарному времени работы. Как определено в Y.1540, коэффициент готовности относится к однонаправленному IP-потоку между определённой парой (или набором) точек измерений MP (Measurement Point). Сеть моделируется как объединение сетевых сегментов, соединённых каналами передачи данных. MP - являются функциональными границами сегмента.

Параметры доставки пакетов IP

В общем, сеанс связи состоит из трёх фаз - установления соединения, передачи информации и разъединения соединения. В рекомендации ITU-T Y.1540 из трёх фаз сеанса связи рассматривается только вторая фаза - фаза доставки IP-пакета. Такой подход отражает природу сетей IP, неориентированных на установление соединений. Спецификацию рабочих характеристик и параметров QoS для двух других фаз (установление и разъединение соединения) планируется провести в дальнейшем. Рекомендация ITU-T Y.1540 определяет следующие параметры, характеризующие доставку IP –пакетов:

- задержка доставки IP-пакета (IP packet transfer delay, IPTD);
- параметр IPTD определяется как время (t2 – t1) между двумя событиями - вводом пакета во входящую точку сети в момент t1 и выводом пакета из выходной точки сети в момент t2, где t2 > t1 и (t2 - t1) < Tmax;
- параметр IPTD определяется как время доставки пакета между источником и получателем для всех пакетов как успешно переданных, так и для пакетов, поражённых ошибками.

Средняя задержка доставки пакета IP – параметр, специфицированный в рекомендации Y.1540, определяется как среднее арифметическое задержек пакетов в выбранном наборе переданных и принятых пакетов. Величина средней задержки зависит от передаваемого в сети трафика и доступных сетевых ресурсов, в частности, от пропускной способности. Рост нагрузки и уменьшение доступных сетевых ресурсов ведут к росту очередей в узлах сети и, как следствие, к увеличению средних задержек доставки пакетов. Речевая информация и, отчасти, видеоинформация является примерами трафика, чувствительного к задержкам, тогда как большинство приложений данных менее чувствительно к задержкам.

Вариация задержки IP-пакета (IP packet delay variation, IPDV)

Параметр IPDV, V_k (входной и выходной) для IP-пакета с индексом k определяется между двумя точками сети (входной и выходной) как разность между абсолютной величиной задержки X_k при доставке пакета с индексом k, и определённой эталонной (или опорной) величиной задержки доставки пакета $d_{1,2}$ для тех же самых сетевых точек: $V_k = X_k - d_{1,2}$. Эталонная задержка доставки пакета $d_{1,2}$ между источником и получателем определяется как абсолютное значение задержки доставки первого пакета между данными сетевыми точками. Флуктуация задержки пакета, или джиттер, проявляется в том, что последовательные пакеты прибывают к получателю в нерегулярные моменты времени. В системах IP-телефонии это, к примеру, ведёт к искажениям звука и в результате к тому, что речь становится неразборчивой.

Коэффициент потери пакетов IP (IP packet loss ratio, IPLR)

Коэффициент IPLR определяется как отношение суммарного числа потерянных пакетов к общему числу принятых пакетов в выбранном наборе переданных и принятых пакетов. Потери пакетов в сетях IP возникают в том случае, когда значение задержек при передаче пакетов превышает нормированное значение, определённое выше как Tmax. Если пакеты теряются, то в режиме передачи данных возможна их повторная передача по запросу принимающей стороны. В системах VoIP пакеты, пришедшие к получателю с задержкой, превышающей Tmax, отбрасываются, что ведет к провалам в принимаемой речи. Среди причин, вызывающих потери пакетов, необходимо отметить рост очередей в узлах сети, возникающий при перегрузках.

Коэффициент ошибочных пакетов IP (IP packet error ratio, IPER)

Коэффициент IPER определяется как суммарное число пакетов, принятых с ошибками, к сумме успешно принятых пакетов и пакетов, принятых с ошибками.

14.4.2 Рекомендация ITU-T Y.1541

Рекомендация ITU-T Y.1541 определяет численное значение параметров, специфицированных в рекомендации Y.1540, для служб, основанных на протоколах IP. Эти параметры являются основной при согласовании между провайдерами сетей, а также конечными пользователями и привайдерами. Нормы на параметры разделены по различным классам QoS, которые определены в зависимости от приложений и сетевых механизмов, применяемых для обеспечения гарантированного качества обслуживания. В таблице 14.1 представлены нормы на определённые выше сетевые характеристики. Значения параметров, приведённые в таблице, представляют собой, соответственно, верхние границы для средних задержек, джиттера, потерь и ошибок пакетов. В рекомендации Y.1541 представлены спецификации набора параметров, связанных с измерением реальных значений сетевых характеристик - периода наблюдений, длины тестовых пакетов, числа пакетов и т.д. В частности при оценке качества передачи пакетов речи в IP - телефонии минимальный интервал наблюдения должен быть порядка 1-20 с при скорости передачи 50 пакетов/с. Рекомендуемый интервал измерений для задержки, джиттера и потерь должен составлять не менее 60 с.

Таблица 14.1. Нормы для характеристик сетей IP с распределением по классам качества обслуживания

Сетевые характеристики	Классы QoS					
	0	1	2	3	4	5
Задержка доставки пакета IP, IPTD	100мс	400мс	100мс	400мс	1с	Н
Вариации задержки пакета IP, IPDV	50мс	50мс	Н	Н	Н	Н
Коэффициент потери пакетов IP, IPLR	1*10-3	1*10-3	1*10-3	1*10-3	1*10-3	Н
Коэффициент ошибок пакетов IP, IPER	1*10-4	1*10-4	1*10-4	1*10-4	1*10-4	Н

Примечание: Н – не нормировано.

Рекомендация Y.1541 устанавливает соответствие между классами качества обслуживания и приложениями:

- Класс 0 – приложения реального времени, чувствительные к джиттеру, характеризуемые высоким уровнем интерактивности (VoIP, видеоконференции);
- Класс 1 – приложения реального времени, чувствительные к джиттеру, (VoIP,

видеоконференции);

- Класс 2 – передача данных, характеризуемая высоким уровнем интерактивности (например, сигнализация);
- класс 3 - передача данных, интерактивные (диалоговые);
- класс 4 - приложения, допускающие низкий уровень потерь и довольно высокий уровень задержки (короткие массивы данных, потоковое видео);
- класс 5 - традиционные применения сетей IP, не представляющие никаких гарантий QoS.

ГЛАВА 15. Сети MPLS

15.1. Принцип работы сети MPLS

Пока группа IETF разрабатывала модели интегрального и дифференцированного обслуживания, было найдено более эффективное решение проблемы обеспечения качества услуг при передаче мультимедийного трафика. Таким решением является многопротокольная коммутация по меткам MPLS (Multiprotocol Label Switching) [31,32], позволяющая передавать интернет-трафик по сети. Сеть MPLS ориентирована на надежный сервис с установлением соединения в отличие от ненадежных дейтаграммных сетей. При рассмотрении использования механизмов в IP-сетях модели IntServ и DiffServ оперируют соответственно в режиме сквозной передачи и на уровне транзитов. MPLS игнорирует протокол IP, так как нет полей заголовка IP-пакета, обрабатываемых в целях обеспечения качества услуг QoS. В технологии MPLS маршрутизация базируется не на адресе назначения, как в IP-сети, а на метках, которые вставляются в начало каждого пакета данных. Метод использования меток во многом близок к виртуальным каналам. Сети X.25, Frame Relay, ATM также устанавливают метки (идентификаторы виртуальных каналов), на основе которых осуществляется коммутация с помощью таблиц маршрутизации. Заголовок метки MPLS, состоящий из четырех байтов, предопределяет сетевой маршрут, который учитывает требуемый уровень QoS.

Заголовок метки MPLS состоит из следующих полей (рис. 15.1):

- метка (20 бит) используется для выбора соответствующего пути коммутации по меткам;
- поле экспериментальных битов (EXP) содержит 3 бита, которые резервированы для дальнейших исследований и экспериментирования. В настоящее время проводится работа, направленная на создание согласованного стандарта использования этих битов для поддержания дифференцированного обслуживания разнотипного трафика и идентификации класса обслуживания. При предоставлении дифференцированных услуг MPLS-сети это поле может указывать определенный класс обслуживания, например, аналогичный классам DiffServ;
- поле MPLS-стека содержит 1 бит и является средством поддержки

иерархической структуры стека меток MPLS. В заголовке последней метки бит , а во всех остальных- бит ;

- время жизни TTL (8 бит) дублирует аналогичное поле IP-пакета, которое является средством сброса пакетов в сети вследствие образования закольцованных маршрутов.

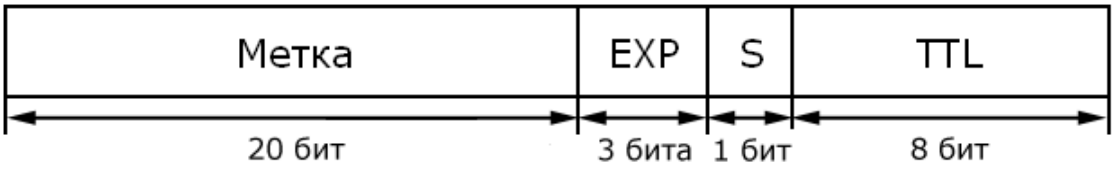


Рис. 15.1. Структура заголовка метки MPLS

Заголовок MPLS-метки не образует полноценного уровня, а «вклинивается» в сетях IP, Ethernet, ATM или Frame Relay между вторым и третьим уровнями модели OSI, оставаясь независимым от этих уровней. В технологии MPLS используются кадры второго уровня для помещения в них пакетов сетевого уровня, которым обычно является IP-пакет.

На рис. 15.2 показано положение заголовка метки в следующих типах кадров: PPP, Ethernet, Frame, Relay, ATM.

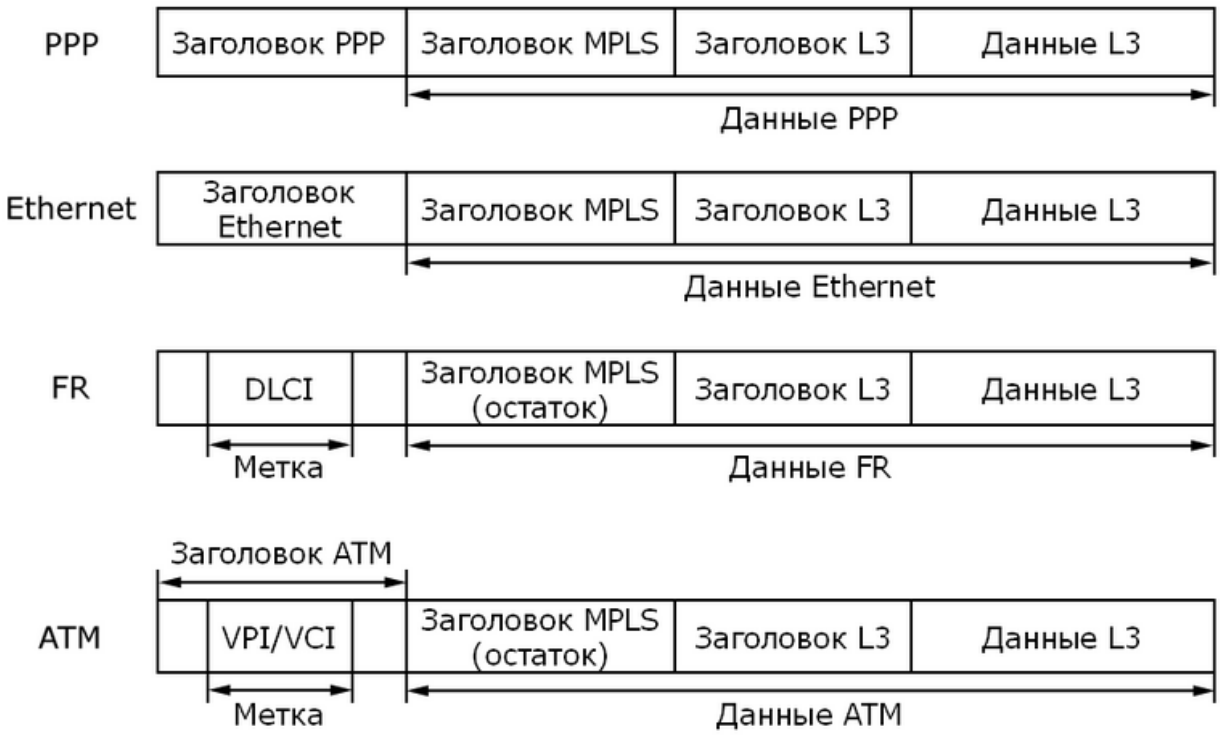


Рис. 15.2. Форматы заголовков нескольких разновидностей технологии MPLS

Одной из сильных сторон технологи MPLS является то, что она может использоваться совместно с различными протоколами уровня 2. Среди этих протоколов – PPP, ATM, Frame Relay, Ethernet. Протокол PPP (Point-to-Point Protocol) применяется для передачи IP-пакетов по коммутируемым и выделенным каналам. PPP является стандартным протоколом Интернета. Он применяется в самых разных случаях, включая обеспечение соединения между маршрутизаторами, между пользователями и провайдерами. В отношении ячеек ATM и кадров Frame Relay для MPLS используются форматы заголовков этих сетей, а во всех остальных случаях – вставку между заголовками второго и третьего уровней. В коммутаторах ATM верхняя метка помещается в поле VPI/VCI заголовка ячейка ATM, а данные о стеке меток MPLS – в поле данных ячеек ATM. Далее для упрощения изложения работы MPLS будем подразумевать, что используется канальный протокол PPP. При разработке протокола PPP за основу был взят другой протокол канального уровня HDLC (High-level Data Link Control, высокоуровневое управление линией связи). Для протокола HDLC характерно его функциональное разнообразие, которое выражается в подмножестве относящихся к нему протоколов. Протокол канального уровня сети X.25 является одним из них и называется сбалансированным протоколом доступа к каналу LAP-B (Link Access Procedure Balanced). Протокол PPP отличается от подмножества протоколов HDLC в следующем.

- Не занимается упорядочиванием кадров и проверкой порядка их следования;
- Производит удаленную аутентификацию по протоколам PAP или CHAP (опционно);
- Поддерживает несколько протоколов сетевого уровня.

В MPLS - сетях пересылка пакетов выполняется коммутаторами. После того, как пакет принят сетью MPLS, обработка пакета больше не требуется. Пакет перемещается в сети, основываясь только на содержании метки MPLS. Поэтому сеть MPLS можно рассматривать для IP-пакета как один транзит. Маршрутизатор с поддержкой MPLS использует содержимое метки MPLS для указания маршрута, основываясь на требованиях приложения к уровню качества обслуживания QoS. Внутри сети MPLS содержимое заголовка IP-пакета больше не нуждается в рассмотрении для определения маршрута. Содержимое метки определяется в соответствии с несколькими критериями, которые объединены в определённый класс эквивалентности пересылки FEC (Forwarding Equivalency Class). Класс FEC может осуществлять сортировку пакетов по различной совокупности значений, в которую могут входить следующие:

- адрес в заголовке IP-пакета;
- номер TCP-порта

и другие. Технология сети MPLS позволяет использовать модель дифференцированного обслуживания DiffServ для обеспечения требований пользователя качеством обслуживании QoS. Поэтому FEC включает классы обслуживания. Они указываются в трех битах EXP заголовка метки, что позволяет реализовать до восьми комбинаций битов. Следует отметить отсутствие стандартизированного протокола реализации DiffServ в сети MPLS. На рисунке 15.3 приведен пример коммутации пакетов в сети MPLS. Под доменом MPLS понимается сеть MPLS, обслуживаемая одним оператором. Рассмотрим работу маршрутизаторов коммутации меток.

15.1.1. Маршрутизатор коммутации меток (LSR)

Маршрутизатор коммутации меток LSR (Label Switching Router) является «двигателем» домена MPLS. Маршрутизатор LSR определяется как любое устройство, способное поддерживать протокол MPLS. LSR может являться IP-маршрутизатором, коммутатором Frame Relay, коммутатором ATM. Технология MPLS поддерживает несколько типов кадров: PPP, Ethernet, Frame Relay и ATM. Это не означает то, что под MPLS работает какая-либо из перечисленных технологий. Это означает только то, что в технологии MPLS

используются форматы кадров этих технологий для помещения в них пакета сетевого уровня, которым почти всегда является IP-пакет. Когда пакет, расширенный за счет заголовка метки MPLS, поступает на маршрутизатор LSR с помощью таблицы маршрутизации и определяется исходящий канал и значение новой метки в пакете. Смена меток производится так же, как и в рассмотренных сетях связи с виртуальными каналами X.25, FR и ATM.

15.1.2. Граничный маршрутизатор коммутации меток (LER)

На границах домена MPLS стоят граничные LSR. Документация по MPLS не делает различий между LSR и граничным LSR за исключением их местоположения в домене. Возникающая в документах путаница, связанная с тем, что оба типа коммутаторов обозначались, как LSR, привела к введению термина Label Edge Router (LER, граничный коммутатор меток), позволяющего отличать граничные LSR от внутренних LSR. Разница между ними заключается в следующем важном моменте: LSR в домене MPLS должны коммутировать пакеты по метке MPLS и понимать протоколы MPLS, в то время как LER должен также поддерживать не имеющие отношения к MPLS функции, такие как обычная маршрутизация по IP-адресу, по крайней мере, для одного порта. Одним из основных отличий MPLS от сетей связи с виртуальными каналами (X.25, FR и ATM) является способ построения таблицы маршрутизации. В сетях с виртуальными каналами пользователь, желающий установить соединение, посылает в адрес получателя сообщение запроса соединения. В результате создаётся путь и соответствующая запись в таблице маршрутизации.

В MPLS вообще отсутствует фаза установления каждого соединения. На рисунке 15.3 приведён пример домена MPLS-сети, состоящий из двух граничных (LER1, LER2) и двух внутренних (LSR1, LSR2) маршрутизаторов коммутации меток. Граничный маршрутизатор выполняет функции назначения и удаления меток (LER1 вставляет метку 1 пакета между заголовком IP и заголовком уровня 2 (L2), а LER2 удаляет метку 4 в этом пакете IP). Путь следования пакетов в сети MPLS определяется тем классом эквивалентности при пересылке FEC, который установлен для этого потока во входном граничном маршрутизаторе LER. Такой путь носит название коммутируемого по меткам тракта LSP (Label-Switched Path) и идентифицируется набором меток во внутренних маршрутизаторах (LSR), расположенных на пути следования потока от отправителя к получателю. Внутренний маршрутизатор коммутирует пакет с меткой от одного интерфейса к другому интерфейсу с заменой метки. LER1 принимает пакет с меткой 1 и отправляет этот пакет LSR2 с меткой 5. LSR2 принимает пакет и отправляет LER2 с меткой 4. Таким образом, метка LER и LSR имеет локальное

значение, как и логические номера виртуальных каналов в сетях ATM, Frame Relay, X.25. Как видно из рисунка 3 продвижение IP-пакета происходит на основе IP-адресной информации той технологии, которую MPLS использует на участке между оконечной станцией и доменом MPLS и на основе меток внутри домена MPLS. L2 здесь означает уровень 2.

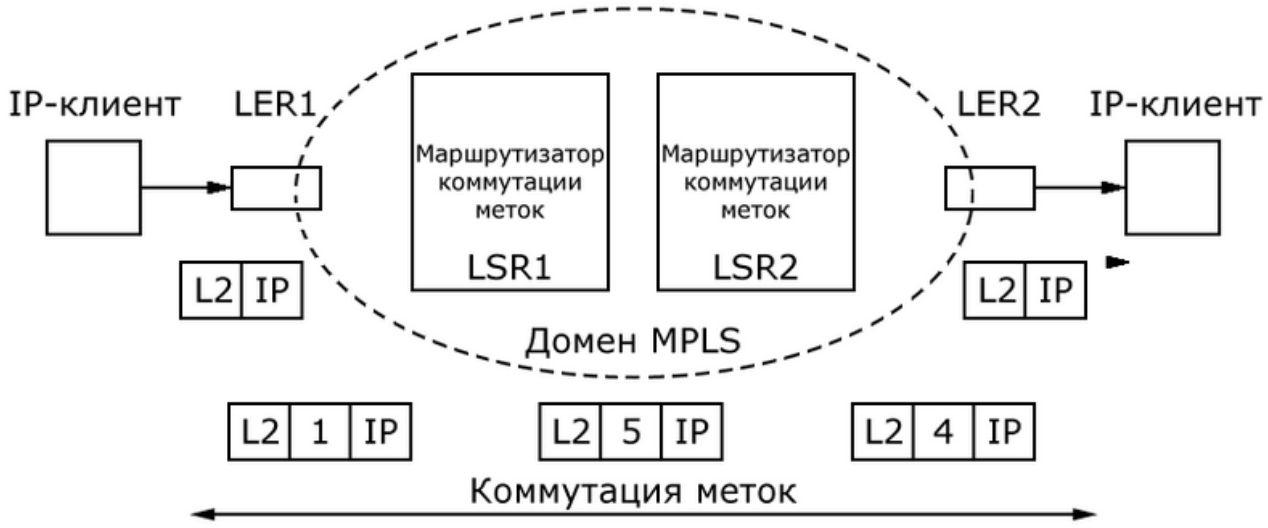


Рис. 15.3. Пример коммутации пакетов «данные»

Кроме функции коммутации, каждый маршрутизатор MPLS выполняет функцию управления по формированию таблицы маршрутизации. Эта таблица называется таблицей пересылки LIB (Label Information Base). LIB состоит из входящей метки и одной или нескольких вложенных записей. Каждая такая запись включает выходную метку, номер выходного интерфейса и адрес следующего маршрутизатора в LSR.

Все узлы MPLS используют протоколы маршрутизации TCP/IP для обмена соответствующей информацией маршрутизации с другими узлами MPLS-сети при создании таблицы LIB. Внутренние LSR коммутируют эти служебные пакеты не по меткам, а по обычным IP-заголовкам. Продвижение кадра в MPLS-сети происходит на основе метки MPLS и техники коммутируемого по меткам тракта LSP, а не на основе адресной информации и той технологии, формат кадра которой использует MPLS. Например, если в MPLS применяется кадр Ethernet, то MAC-адреса источника и приемника, хотя и присутствуют в соответствующих полях Ethernet, но для продвижения кадра не задействуются.

15.2. Стек меток

Функциональные возможности стека MPLS позволяют реализовать несколько

функций и, в частности, объединить (агрегировать) несколько LSP в один. Концепция стека меток является развитием концепции двухуровневой адресации виртуальных каналов VPI/VPC, принятой в ATM. Многоуровневый принцип создания путей сокращает время задержки передачи пакета.

Если в одном LSP сливается несколько потоков (каждый поток – со своим FEC и своей меткой), то этот LSP помещает сверху метку нового FEC, который соответствует объединенному потоку пакетов, образующемуся в результате слияния. В точке окончания такого объединенного тракта он разветвляется на составляющие его индивидуальные LSP. Так могут объединяться тракты, имеющую общую часть маршрута. Пример четырёхуровнего стека меток приведён на рисунке 15.4.

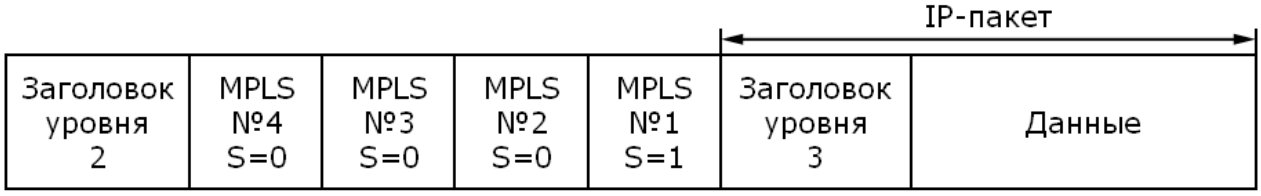


Рис. 15.4. Пример четырёхуровнего стека меток MPLS

Здесь заголовок MPLS № 1 был первым заголовком MPLS, помещённым в пакет, затем в него были помещены заготовки № 2, № 3, № 4. Извлекаются заголовки меток из стека в обратной последовательности (4,3,2,1). Коммутация по меткам всегда использует верхнюю метку стека, метки удаляются из пакета сверху. Каждый заголовок MPLS имеет собственные значения поля EXP, S-бита и поля TTL. Заголовок метки №1 на рисунке 15.4 является самым нижним (S=1). MPLS может выполнять со стеком следующие операции: помещение метки в стек (push), удаление верхней метки из стека (pop), замену метки (swap). На рисунке 15.5 показан пример использования стека в MPLS при создании путей двух пакетов IP с разными адресами назначения и, соответственно, разными значениями FEC. Сеть состоит из двух MPLS - доменов. В LER1 начинаются два пути (коммутируемых по меткам тракта) - LSP1 и LSP2 (LSP1 для пакета IP_1 с адресом получателя A в заголовке и LSP2 для пакета IP_2 с адресом получателя B в заголовке). В LER1 метки каждого из этих пакетов (соответственно 305 для первого пакета и 14 - для второго пакета) проталкиваются (push) вниз, а верхней становится в обоих пакетах метка 256. Продвижение обоих пакетов производится по верхней метке, которая на выходе меняет значение (256 на 272).

На предпоследнем LSR2 домене производится удаление (pop) верхней метки. В результате

верхней меткой для пакета IP_1 становится метка 305, а для IP_2 метка 14 уничтожается. LER2 завершает путь LSP2 пакета IP1, передавая его оконечному устройству. LER2 продвигает пакет IP_1 на основе таблицы маршрутизации. LER2 заменяет метку 305 на метку 299 и далее через LER3 и LER4 продвигает его по пути LER2 до оконечного пункта А. Приведённый пример двухуровневого пути может быть расширен для любого количества уровней.

Таким образом, если в одном маршрутизаторе сливаются несколько потоков (каждый поток со своим FEC и со своей меткой), то этот коммутируемый по меткам тракт (путь) LSP не заменяет метки, связанные с названными потоками, а оставляет их, помещая сверху метку нового FEC, который соответствует объединенному потоку пакетов, образующемуся в результате слияния. Если в промежуточном маршрутизаторе такого объединенного потока происходит слияние еще с одним потоком, то на верху стека устанавливается еще одна метка. Путь LSP1: LERl, LSRl, LSR2, LER2, LER3, LSR3, LER4 пакета IP1 с адресом получателя пункт А. Путь LSP2: LER1, LSR1, LSR2, LER 2 пакета IP2 с адресом получателя пункт В. В результате стек меток позволяет создать древовидную структуру множества трактов LSP, заканчивающихся в одном маршрутизаторе (корне дерева).

Введем понятие уровня m тракта LSP. Маршрут LSP уровня m представляет собой последовательность маршрутизаторов, которая с входного LSR, помещающего в пакет метку уровня m (стек из m заголовков меток), содержит промежуточные LSR, каждый из которых принимает решение о пересылке пакета на основе метки уровня m и заканчивается входным LSR, где решение о пересылке принимается на основе метки уровня m-1 или на основе обычных (не MPLS, а IP) процедур пересылки. От предпоследнего LSR в выходной граничный маршрутизатор можно передавать пакеты со стеком метки глубины (m-1), поскольку метка уровня m выходному LSR не требуется. В предпоследнем LSR производится уничтожение верхней метки стека.

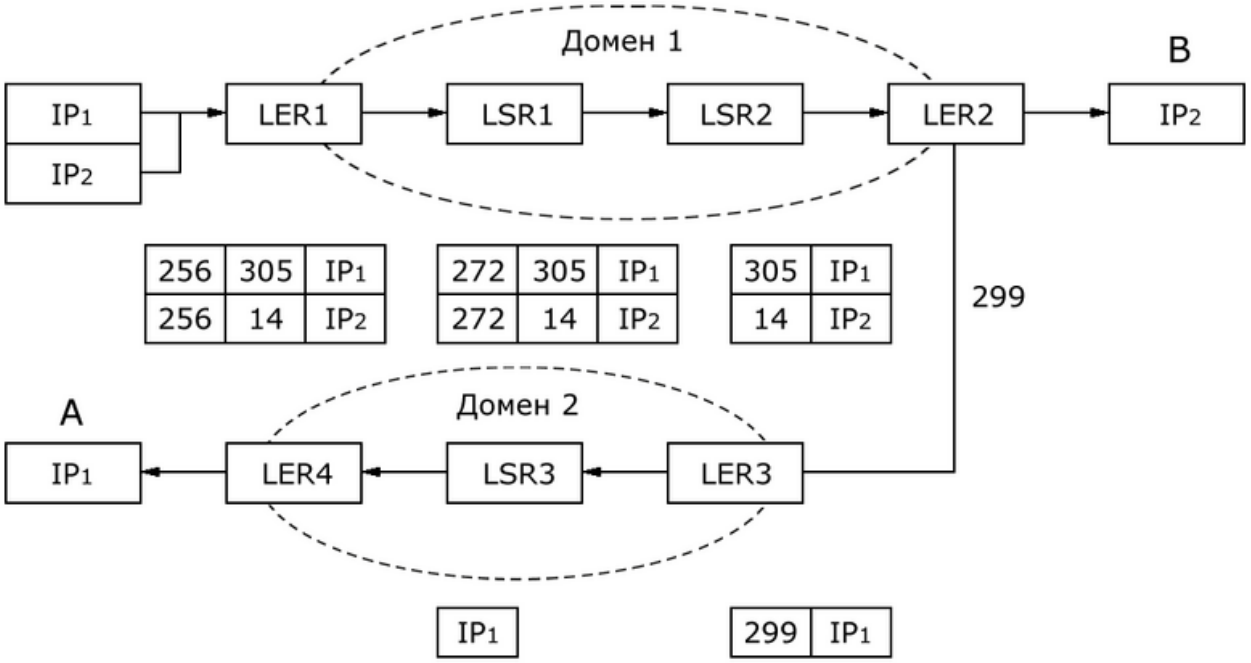


Рис. 15.5. Пример путей LSP1 и LSP2, проложенных в доменах 1 и 2

На рис. 15.6 приведен пример древовидной структуры множества трактов LSP четырёх уровней (m=4).

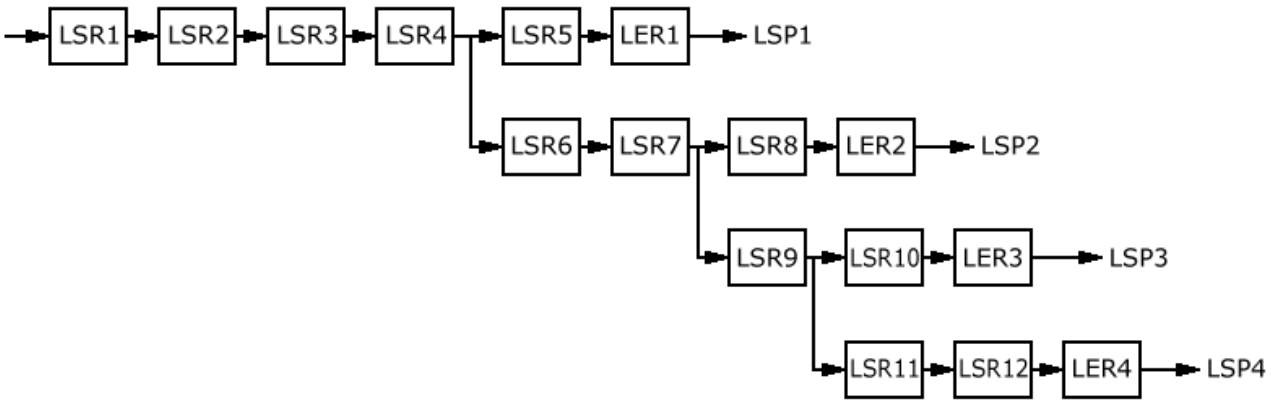


Рис. 15.6. Древовидная структура трактов LSP
В таблице 15.1 приведена структура этих уровней в маршрутизаторах LSR1, LSR2, LSR3, LSR4.

Таблица 15.1. Структура стека меток тракта LSP4

Уровни LSP	Содержание метки

4	Общая метка LSP1, LSP2, LSP3, LSP4
3	Общая метка LSP2, LSP3, LSP4
2	Общая метка LSP3, LSP4
1	Метка LSP4

Аналогично для LSP3, LSP2, LSP1 древовидная структура представляет соответственно три (для LSP3) и два (для LSP1 и LSP2) уровня тракта LSP.

15.3. Маршрутизация пакетов в узле коммутации LSR

Когда пакет MPLS поступает в маршрутизатор коммутации по меткам LSR, этот маршрутизатор производит коммутацию пакета, используя имеющуюся у него таблицу информационной базы меток LIB (Label Information Base). Ниже приведён пример такой таблицы пересылки пакета в MPLS (табл. 15.2).

Таблица 15.2. Пример таблицы пересылки LIB

Входящая метка	Первая запись	Вторая запись
Значение входящей метки	Исходящая метка	Исходящая метка
	Выходной интерфейс	Выходной интерфейс
	Адрес следующего LSR	Адрес следующего LSR

Как видно из таблицы 15.2, пересылка пакета производится на выходной интерфейс на основании значения метки во входящем в LSR пакете MPLS. При этом в исходящем из LSR пакете указывается адрес следующего LSR и устанавливается новое значение метки. Несколько записей в таблице пересылки (в табл. 15.2 их две) требуются при многоадресной рассылке пакета. Программное обеспечение LSR может быть разработано в одном из двух вариантов LIB – либо одна общая таблица для LSR, либо их несколько по количеству интерфейсов LSR. Алгоритм формирования привязки метки к FEC предусматривает

выделение в LSR отдельного пула «свободных» меток. Эти метки используются для их локальной привязки, а число таких «свободных» меток определяет максимальное число таких пар «метка – FEC», которое может быть установлено в текущий момент работы данного LSR.

15.4 Распределение меток

Сущность распределения меток – информировать смежные маршрутизаторы о привязке «FEC-метка». Выбор маршрута заключается в определении пути LSP для данного кода эквивалентности при пересылке FEC. Фактическая установка LSP заключается в двух типах привязки меток к FEC. При первом типе метка выбирается и назначается в LSR локально. При втором типе LSR получает от некоторого смежного LSR информацию о привязке метки, которая создана на нем. Такую привязку называют удаленной. Локальная и удаленная привязка распространяется только между смежными маршрутизаторами LSR. При локальной привязке маршрутизатор информирует назначенную метку данному классу FEC смежным LSR. Эти смежные LSR получают возможность правильно установить метки в пакеты, направленные LSR-создателю этой метки. При удаленной привязке создателем «FEC-метка» является LSR транзитного участка тракта LSP. Это позволит производить замену входящей на исходящую метку в пакетах, передаваемых LSR-создателем привязки. Таким образом, метки могут рассматриваться как в определенной степени аналог идентификаторам логических номеров виртуальных каналов глобальных сетей X.25 (LCN), FR (DLCI), ATM (VPI/VCI). Архитектура MPLS позволяет использовать следующие протоколы распределения меток:

- специальный протокол распределения меток LDP (Label Distribution Protocol), подлежащий рассмотрению в следующем разделе;
- расширение возможностей протокола IP-сети BGP;
- расширение возможностей протокола IP-сети RSVP.

15.4.1 Протокол распределения меток LDP

В сети MPLS в отличие от сетей связи X.25, FR, ATM (VPI/VCI) с виртуальными каналами отсутствует фаза установления соединения по сообщению запроса пользователя. Метки в коммутируемом по меткам тракте LSP назначаются с помощью протокола распределения меток LDP (Label Distribution Protocol), причём существуют разные способы такого распределения. Процедуры протокола LDP позволяют создать тракт LSP. Создание LSP означает создание таблиц коммутации по меткам во всех маршрутизаторах этого LSP. Функция протокола LDP состоит в частности, в определении каждой привязки «FEC - метка» в каждом LSR тракта LSP. Один из вариантов работы LDP состоит в следующем. При загрузке маршрутизатора выявляется, для каких маршрутов он является пунктом назначения (например, какие хвосты находятся в его локальной вычислительной сети). Для них создаётся один или несколько FEC и каждому из них выделяется метка, значение которой сообщается соседним LER. Эти LER. в свою очередь, заносят эти метки в свои таблицы пересылки и посылают новые метки своим соседним маршрутизаторам. Процесс продолжается до тех пор пока все маршрутизаторы не получат данные о маршрутах. По мере формирования путей могут резервироваться ресурсы, что позволяет обеспечить надлежащее качество обслуживания. Протокол LDP является протоколом прикладного уровня и использует оба протокола транспортного уровня - UDP и TCP (рис. 15.7).

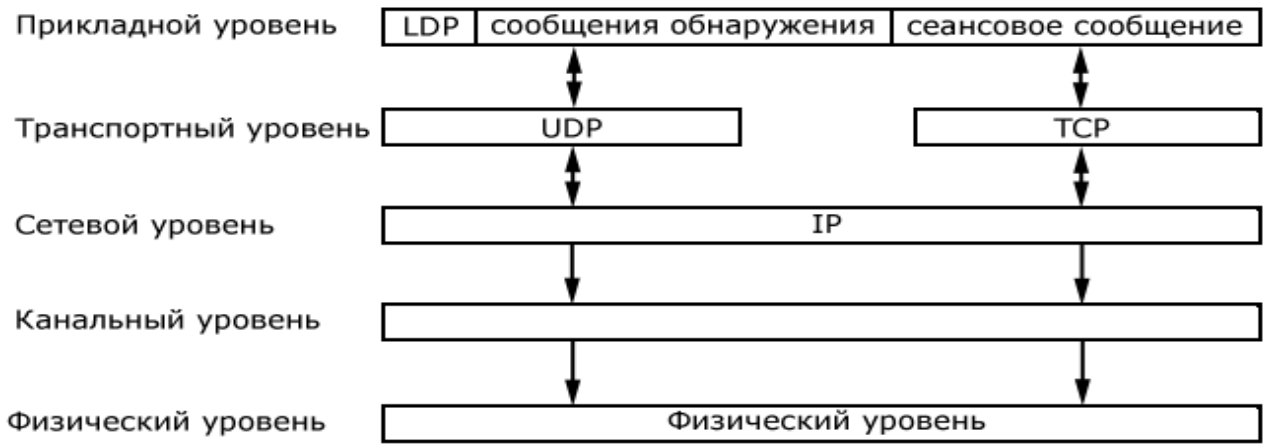


Рис. 15.7. Стек протоколов при обмене сообщениями по протоколу LDP

Протокол LDP работает с использованием транспортного уровня по протоколу UDP только для передачи сообщения обнаружения DISCOVERY. При этом используются

сообщения многоадресной рассылки Hello для получения информации о смежных с ним LSR. После обмена этими сообщениями устанавливается TCP-соединение и сеанс LDP с этими маршрутизаторами. Теперь MPLS позволяет LSR запросить у смежного LSR информацию о привязке «FEC-метка». Такой режим называется нисходящее распределение меток по требованию. Для этого LSR запрашивает метку, передав сообщение Label Request. В последнее сообщение входит FEC, для которого запрашивается метка. Если сообщение Label Request поступает в выходной граничный маршрутизатор, то в нем содержится метка, которая имеет локальное значение на участке между входным и соседним с ним вышестоящим маршрутизатором. Если на всех следующих далее вышестоящих LSR успешно произойдет привязка меток к FEC, то после обработки во входном LER сообщения Label Mapping, полученного от соседнего с ним нижестоящего маршрутизатора, маршрут для тракта LSP будет создан.

Назначение меток производится в сторону отправителя трафика, то есть противоположную направлению трафика. Такой LSR, где назначается метка, называется нижним (расположен «ниже по течению»), а расположенный «выше по течению» верхним LSR. Метка всегда локальна, то есть обозначает некоторый FEC для пары маршрутизаторов, между которыми имеется прямая или коммутируемая связь. Напомним, что значения идентификатора виртуального пути VPI и виртуального канала VCI в сети ATM являются также локальными. Пересылка пакета данных MPLS с FEC, соответствующим установленной метке, производится от верхнего LSR к нижнему LSR. Для пересылки пакетов данных того же FEC к следующему маршрутизатору LSR используется другая метка, идентифицирующая этот FEC для новой пары маршрутизаторов, в которой маршрутизатор, бывший в предыдущей паре нижним, приобретает статус верхнего, а статус нижнего получает второй маршрутизатор этой новой пары. Отсюда ясно, что каждый маршрутизатор MPLS-сети, должен хранить соответствие между входящими и исходящими метками для всех FEC, которыми он оперирует. Напомним, что длина поля метки составляет 20 бит и означает, что маршрутизатор одновременно может оперировать 2^{20} метками, которым соответствует определённые FEC.

15.5 Инжиниринг трафика

Инжиниринг трафика TE (Traffic Engineering) представляет функции мониторинга и управления трафиком с тем, чтобы обеспечить нужное качество обслуживания путём рационального использования сетевых ресурсов за счет сбалансированной их загрузки. Этому английскому термину TE соответствует управление разнотипным трафиком в MPLS, отмечая связь рассматриваемых здесь механизмов с задачей обеспечивать разное качество обслуживания QoS трафика разных типов.

Принятая в MPLS технология TE, позволяет снять ограничения, присущие протоколам маршрутизации в IP-сетях. Задача максимального использования ресурсов для IP-сетей, лежащих в основе Интернета, не была первоочередной, т.к. Интернет не считался долгое время коммерческой сетью. Поэтому в сетях MPLS необходимо было изменить традиционные подходы к выбору маршрутов.

Известно, что все протоколы маршрутизации (RIP, OSPF и другие), выбирают для трафика, направленного в определенную сеть, кратчайший маршрут в соответствии с некоторой метрикой. Выбранный путь может быть более рациональным, например, если в расчёт метрики принимается номинальная пропускная способность каналов связи и менее рациональным, если учитывается только количество промежуточных маршрутизаторов (хопов) между исходной и конечной подсетями. Однако в любом из случаев выбирается единственный маршрут, даже если существует несколько альтернативных путей. Примером неэффективности является IP-сеть сеть с топологией, приведённой на рисунке 15.8. Недостаток методов маршрутизации трафика в IP - сетях заключается в том, что пути выбираются без учета текущей загрузки ресурсов сети. Даже если кратчайший путь уже перегружен, пакеты всё равно посылаются по этому пути. Так, в сети, представленной на рисунке 15.8, верхний путь будет продолжать использоваться даже тогда, когда его ресурсов перестанет хватать для обслуживания трафика от A к E, а нижний путь будет простаивать, хотя, возможно, ресурсов маршрутизаторов B и C хватило бы для более качественной передачи трафика. Отсюда видна неэффективность методов распределения ресурсов сети - одни ресурсы работают с перегрузкой, а другие не используются вовсе.

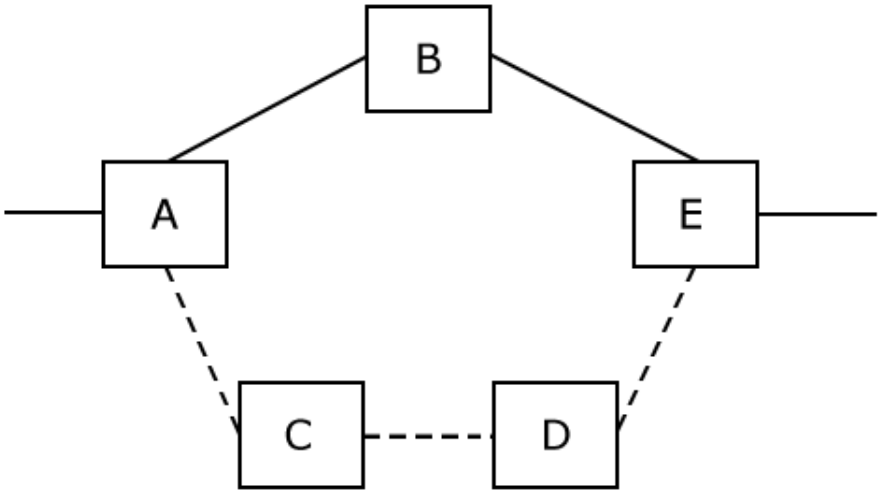


Рис. 15.8. Неэффективность кратчайшего пути

Применение в MPLS механизма инжиниринг трафика TE позволяют решить эту проблему, указав два разных пути от маршрутизатора A к маршрутизатору E, то есть кроме A-B-E маршрут A-C-D-E. TE лучше использует сетевые ресурсы за счёт перевода части трафика с более загруженного на менее загруженный участок сети. При этом достигается более высокое качество обслуживания трафика, поскольку уменьшается вероятность перегрузки в сети. Кроме того, для услуг, которые требуют выполнения заданных норм качества обслуживания QoS (например, заданного коэффициента потерь пакетов, задержки, джиттера) инжиниринг трафика позволяет обеспечить надлежащее QoS путём назначения явно определённых маршрутов.

В технологии MPLS TE пути LSP называют TE-туннелями. TE-туннели не прокладываются распределенным способом вдоль путей, находимых обычными протоколами маршрутизации независимо в каждом отдельном устройстве LSR. Вместо этого TE-туннели прокладываются в соответствии с техникой маршрутизации от источника, когда централизовано задаются промежуточные узлы маршрута. В этом отношении TE-туннели подобны PVC-каналам в технологиях ATM и Frame Relay. Инициатором задания маршрута для TE-туннеля выступает начальный узел туннеля, а рассчитываться такой маршрут может как этим же начальным узлом, так и внешней по отношению к сети программной системой или администратором.

MPLS TE поддерживает туннеля двух типов:

- Строгий TE-туннель – определяет все промежуточные узлы между двумя пограничными устройствами;
- Свободный TE-туннель – определяет только часть промежуточных узлов от одного пограничного устройства до другого, а остальные промежуточные узлы выбираются

устройством LSR самостоятельно.

На рисунке 15.9 показаны оба типа туннелей. Туннель 1 является примером строгого туннеля, при его задании внешняя система (или администратор сети) указана как начальный и конечный узлы туннеля, так и все промежуточные узлы, то есть последовательность IP-адресов для устройств LER1, LSR1, LSR2, LSR3, LSR4, LER3. Таким образом, внешняя система решила задачу инжиниринга трафика, выбрав путь с достаточной неиспользуемой пропускной способностью. При установлении туннеля 1 задается не только последовательность LSR, но и требуемая пропускная способность пути. Несмотря на то, что выбор пути происходит в автономном режиме, все устройства сети вдоль туннеля 1 проверяют, действительно ли они обладают запрошенной неиспользуемой пропускной способностью, и только в случае положительного ответа туннель прокладывается.

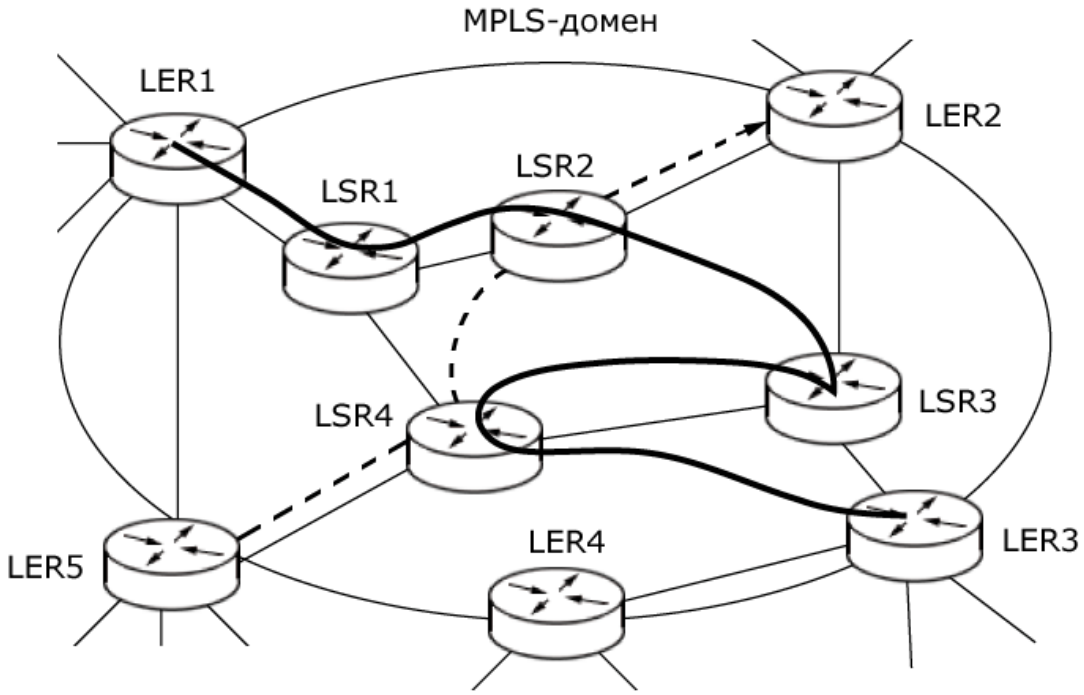


Рис. 15.9. Два типа E-туннелей в технологии MPLS

При прокладке туннеля 2 (свободного) администратор задает только начальный и конечный узлы туннеля, то есть устройства LER5 и LER2. Промежуточные устройства LSR4 и LSR2 находятся автоматически начальным узлом туннеля 2, то есть устройством LER5, а затем с помощью сигнального протокола устройства LER5 сообщает этим и конечному устройствам о необходимости прокладки туннеля.

Независимо от типа туннеля он всегда обладает таким параметром, как резервируемая средняя пропускная способность. В нашем примере туннель 1 резервирует для трафика 10

Мбит/с, а туннель 2 резервирует 36 Мбит/с. Эти значения определяются администратором, и технология MPLS TE никак не влияет на их выбор, она только реализует запрошенное резервирование. Чаще всего администратор оценивает резервируемую для туннеля пропускную способность на основании измерений трафика в сети, тенденций изменения трафика. Некоторые реализации MPLS TE позволяют затем автоматически корректировать величину зарезервированной пропускной способности на основании трафика, проходящего через туннель.

Методы инжиниринга трафика чаще применяют не к отдельным, а к агрегированным потокам, которые являются объединением нескольких потоков. Так как мы ищем общий маршрут для нескольких потоков, то агрегировать можно только потоки, имеющие общие точки входа и выхода. Агрегированное задание потоков позволяет упростить задачу выбора путей, так как при индивидуальном рассмотрении каждого пользовательского потока промежуточные коммутаторы должны хранить слишком большие объемы информации, поскольку индивидуальных потоков может быть очень много. Необходимо подчеркнуть, что агрегирование отдельных потоков в один возможно только в том случае, когда все потоки, составляющие агрегированный поток, предъявляют одни и те же требования к качеству обслуживания.

Однако сама по себе прокладка в MPLS-сети TE-туннеля еще не означает передачи по нему трафика. Она означает только то, что в сети действительно существует возможность передачи трафика по туннелю со средней скоростью, не превышающей зарезервированное значение. Для того чтобы данные были переданы по туннелю, администратору предстоит еще одна ручная процедура – задание для начального устройства туннеля условий, определяющих, какие именно пакеты должны передаваться по туннелю. Такими условиями могут быть классы эквивалентности пересылки FEC и классы обслуживания. Устройство LER должно сначала провести классификацию трафика, удостоверившись, что средняя скорость потока не превышает зарезервированную, а затем начать маркировать пакеты, используя начальную метку TE-туннеля, чтобы передать трафик через сеть MPLS.

Для выбора и проверки TE-туннелей используются расширенный протокол маршрутизации OSPF-TE, который распространяет следующую информацию:

- максимальная пропускная способность звена (то есть между маршрутизаторами);
- максимальная пропускная способность звена, доступная для резервирования;
- резервированная на звене пропускная способность;

- текущее использование пропускной способности звена.

Располагая такими значениями, а также параметрами потоков, для которых нужно определить TE-туннели, маршрутизатор LER может найти решение наиболее рационального использования ресурсов сети. В качестве критерия для этого используется обычно значение min (max Ki) для всех возможных путей.

В общем случае администратору необходимо проложить несколько туннелей для различных агрегированных потоков. С целью упрощения задачи оптимизации выбор путей для этих туннелей обычно осуществляется по очереди, причем администратор определяет очередность на основе своей интуиции. Очевидно, что поиск TE-путей по очереди снижает качество решения – при одновременном рассмотрении всех потоков в принципе можно было бы добиваться более рациональной загрузки ресурсов. Покажем это на примере.

15.5.1. Пример выбора путей

В примере, показанном на рисунке 15.10, ограничением является максимально допустимое значение коэффициента использования ресурсов, равное 0,65. В варианте 1 решение было найдено при очередности рассмотрения потоков 1, 2, 3. Для первого потока был выбран путь A-B-C, так как в этом случае он, с одной стороны, удовлетворяет ограничению (все ресурсы вдоль пути – каналы A-B, B-C и соответствующие интерфейсы маршрутизаторов оказываются загруженными на 50/155=0,32). Пропускная способность каналов A-B и B-C равна B=155, а каналов A-D, D-E, E-C равна B=100. Для второго потока также был выбран путь A-B-C, так как и в этом случае ограничение удовлетворяется - результирующий коэффициент использования оказывается равным 50+40/155=0,58. Третий поток направляется по пути A-D-E-C и загружает ресурсы каналов A- D, D-E и E-C на 30/100=0,3. Решение 1 можно назвать удовлетворительным, так как коэффициент использования любого ресурса в сети не превышает 0,58.

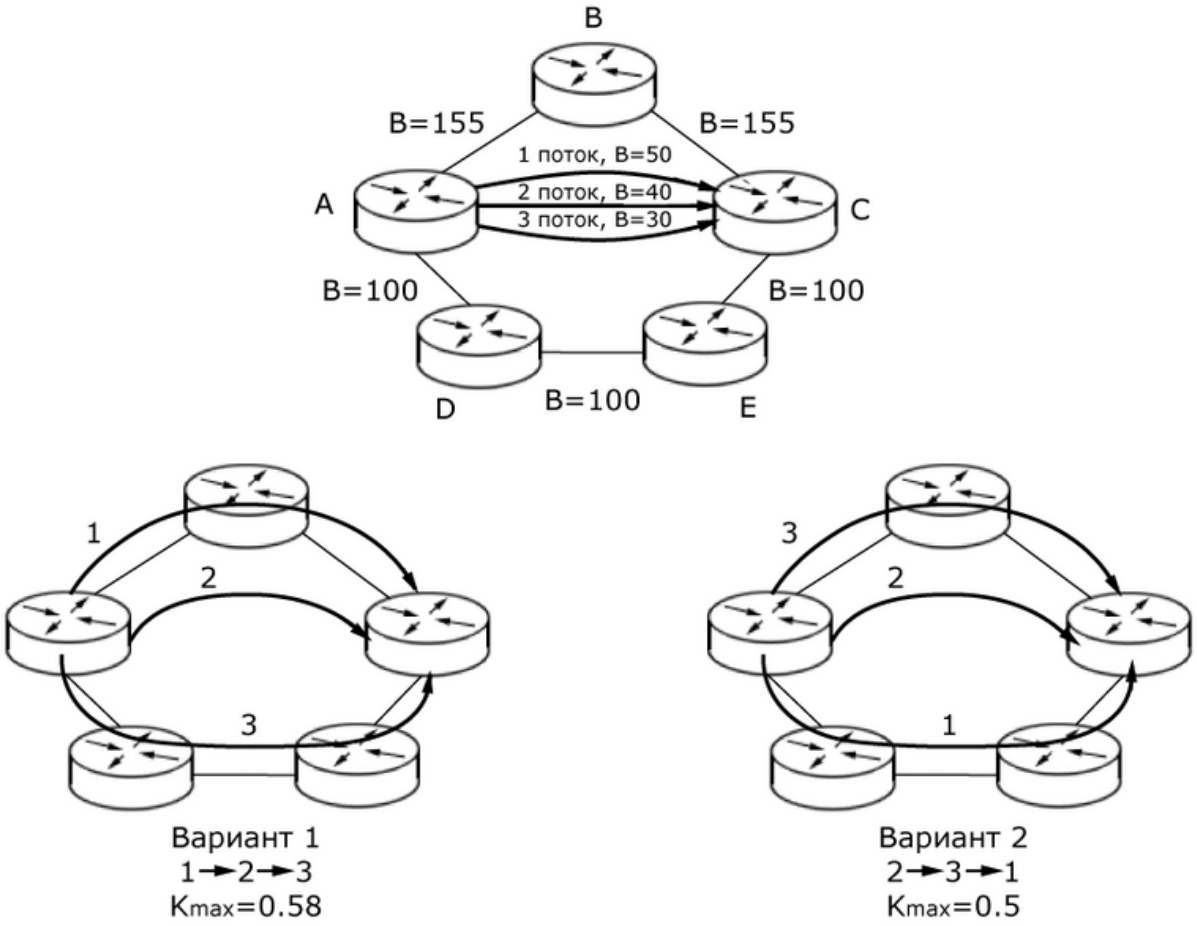


Рис. 15.10. Зависимость коэффициента использования ресурсов сети от стратегии выбора туннелей

Однако существует лучший способ, представленный в варианте 2. Здесь потоки 2 и 3 были направлены по верхнему пути А-В-С, а поток 1 по нижнему А-Д-Е-С. Ресурсы верхнего пути оказываются загруженными на 0,45, и нижнего - на 0,5, то есть на лицо более равномерная загрузка ресурсов, а максимальный коэффициент использования всех ресурсов сети не превышает 0,5. Этот вариант может быть получен при одновременном рассмотрении всех трех потоков с учетом ограничения min (max Ki) или же при рассмотрении потоков по очереди в последовательности 2, 3 ,1.

Несмотря на не оптимальность решения, в производимом сегодня оборудовании применяется вариант технологии MPLS TE с последовательным рассмотрением потоков. Он проще в реализации и ближе к стандартным для протоколов OSPF процедурам нахождения кратчайшего пути по одной сети назначения. В отсутствие ограничений найденное решение для выбора кратчайших путей не зависит от последовательности учета сетей, для которых производится поиск. Кроме того, при изменении ситуации – появлении новых потоков или изменении интенсивности существующих – найти путь удается только для одного потока.

В технологии MPLS TE информация о найденном рациональном пути используется полностью, то есть запоминаются IP-адреса источника, всех транзитных маршрутизаторов и конечного узла. Поэтому достаточно, чтобы поиском путей занимались только пограничные устройства сети (LER), а промежуточные устройства (LSR) лишь поставляли им информацию о текущем состоянии резервирования пропускной способности каналов. После нахождения пути независимо от того, найден он был устройством LER или администратором, его необходимо зафиксировать. Для этого в MPLS TE используется расширение уже рассмотренного нами протокола резервирования ресурсов (RSVP), который часто в этом случае называют протоколом RSVP TE.

Для реализации этой функции RSVP-TE расширяется новым объектом- ERO (Explicit Route Object). Объект переносится в сообщении Path и содержит явно заданный маршрут, по которому должно идти сообщение. Пересылка такого сообщения маршрутизатором определяется не адресом получателя, содержащимся в заголовке IP-пакета, а содержанием объекта ERO. Эта функция позволяет автоматически (или в результате действий администратора) ремаршрутизировать LSP в обход перегружаемых областей. При установлении нового пути в сигнальном сообщении наряду с последовательностью адресов пути указывается также и резервируемая пропускная способность. Каждое устройство LSR, получив такое сообщение, вычитает запрашиваемую пропускную способность из пула свободной пропускной способности соответствующего интерфейса, а затем объявляет остаток в сообщениях протокол маршрутизации, например OSPF. Таким образом, протокол RSVP-TE выполняет свою традиционную функцию обеспечения требований QoS пользователей в соответствии с моделью интегрального обслуживания.

В заключение рассмотрим вопрос отношения технологий MPLS TE и QoS. Как видно из описания, основной целью MPLS TE является использование возможностей MPLS для достижения внутренней цели поставщика услуг, а именно сбалансированной загрузки всех ресурсов сети. Однако при этом так же создается основа для предоставления транспортных услуг с гарантированными параметрами QoS, так как трафик по TE-туннелям передается при соблюдении некоторого максимального уровня коэффициента использования ресурсов. Коэффициент использования ресурсов оказывает решающее влияние на процесс образования очереди, так что потоки, передаваемые по TE-туннелям, передаются с некоторым гарантированным уровнем QoS.

Для того чтобы обеспечить параметры QoS для разных видов трафика, поставщику услуг необходимо для каждого класса эквивалентности пересылки установить в сети отдельную

систему туннелей. При этом для чувствительного к задержкам FEC требуется выполнить резервирование таким образом, чтобы максимальный коэффициент использования ресурсов туннеля находился в диапазоне 0,2-0,3, иначе задержки пакетов и их вариации выйдут за допустимые пределы.

15.6. Быстрая ремаршрутизация

Кроме основной задачи гибкого управления трафиком подсистема TE выполняет с помощью стека меток ещё одну функцию – быструю ремаршрутизацию FRR (Fast Reroute). В случае выхода из строя канала связи в сетях с коммутацией пакетов требуется повторное установление соединения с оконечного пункта. При этом происходят задержки и потери пакетов (ячеек, кадров) данных, значительно влияющих на показатели QoS. FRR в MPLS-сети обеспечивает защиту от этих потерь, ремаршрутизируя трафик, проходящий по LSP, в обход повреждённого канала в течении 50 мсек. Приведённый на рис. 15.11 пример показывает, каким образом FRR используется.

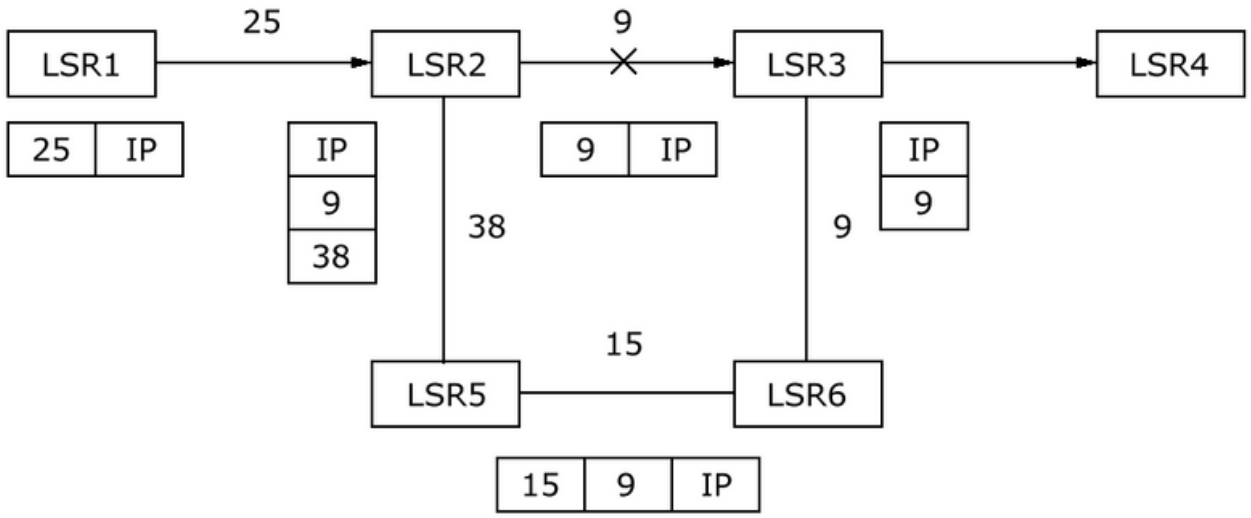


Рис. 15.11. Пример применения FRR.

Как видно из рис. 15.11, когда LSR2 обнаружит, что канал между LSR2 и LSR3 неисправен, трафик в LSR3 будет переведён на резервный туннель (через LSR5 и LSR6). Это выполняется помещением метки 38 наверх стека с помощью процедуры push. Предварительно производится процедура замены метки (swap) 25 на 9. Продвижение пакета через LSR5 происходит по верхней метке. На LSR6 верхняя метка удаляется. В результате верхней меткой, по которой происходит коммутация, становится метка 9, т.е. та же самая, что и в случае исправного канала между LSR2 и LSR3 (т.е. когда в LSR2 метка 25 заменяется на метку 9).

15.7. Преимущества MPLS по сравнению с IP-сетью

Кратко сформулируем преимущества MPLS-сети по сравнению с транспортной IP-сетью.

1. Технология MPLS поддерживает показатели качества обслуживания QoS, предоставляя различные классы обслуживания. IP-сети не предоставляют такой возможности.
2. Технология MPLS позволяет сбалансировать нагрузку в сети, осуществляя перераспределение потоков (инжиниринг трафика). Это повышает показатели QoS за счет оптимизации использования полосы пропускания на недостаточно загруженных маршрутах. Протоколы IP-сети такой возможности не предусматривают.
3. При использовании технологии MPLS провайдеры служб могут создавать виртуальные частные сети VPN. VPN-сети содержат географически удаленные друг от друга узлы, которые могут безопасно связывать их по совместно используемой магистрали. В отличие от IP-сетей технология MPLS позволяет создавать VPN-сети без необходимости использовать дорогостоящее шифрование. Подробно построению VPN-сетей на базе MPLS посвящена следующая глава.

4. Быстрая ремаршрутизация при отказах в каналах связи.

ГЛАВА 16. Виртуальные частные сети на базе MPLS

16.1. Туннелирование MPLS

В технологии MPLS виртуальные частные сети VPN создаются с помощью туннелей. В отличие от VPN IP-сети в MPLS туннели создаются в результате использования стека меток.

Сказанное в предыдущей главе про коммутируемый по меткам тракт LSP уровня m справедливо и по отношению к LSP-туннелю.

В примере на рисунке 15.5 (глава 15) участок пути между LERl LER2 (LERl-LSR1-LSR2-LER2) является LSP-туннелем для пути пакета IP1 между LER1 и LER4, проходящего через семь маршрутизаторов (LERl-LSR1-LSR2-LER2-LER3-LSR3-LER4).

LSP-туннель представляет собой последовательность маршрутизаторов, где первый маршрутизатор является входным, а последний - выходным конечным пунктом. Чтобы направить пакет в LSP-туннель, маршрутизатор входного конечного пункта туннеля помещает метку, назначенную для этого туннеля, наверх существующего в пакете стека меток. Как видно из указанного рисунка, предпоследний маршрутизатор (LSR2) может уничтожить верхнюю метку в стеке до передачи пакета к выходному конечному пункту (LER2). В пределах одного LSP может быть создано несколько LSP-туннелей одного уровня с несовпадающими входными и/или выходными конечными пунктами. Например, в домене 2 может быть создано ещё один или несколько туннелей для LSP2 (при условии, что промежуточных LSR для этого тракта будет не один, а несколько). Внутри любого из LSP-туннелей можно создавать LSP-туннели следующего уровня, что обеспечивает иерархичность организации туннеля. Напомним, что стек меток MPLS организован по принципу последним пришёл - первым вышел LIFO (last-in, first-out), то есть метка, установленная последней, находится наверху стека, и только она обрабатывается при пересылке пакета. Значение бита S=1, установленное в заголовке метки показывает, что эта метка в стеке меток является самой нижней.

16.2. Виртуальная частная сеть MPLS третьего уровня (MPLS L3VPN)

В настоящем разделе рассмотрим построение виртуальных частных сетей на базе технологии MPLS (MPLS L3VPN). При этом доставка элемента данных протокола PDU от клиента до граничного маршрутизатора сети MPLS осуществляется с помощью пакета

технологии IP (третий уровень согласно модели OSI).

16.2.1. Общая модель MPLS L3VPN

На рисунке 16.1 приведён пример общей модели MPLS L3VPN, состоящей из трёх виртуальных частных сетей VPN: VPN A, VPN B, VPN C.

Ядро MPLS L3VPN состоит из внутренних маршрутизаторов провайдера P (Provider router) в магистральной сети (Backbone Network) MPLS и граничных маршрутизаторов провайдера PE (Provider Edge router). В общем случае в корпоративной сети может быть несколько территориально обособленных подсетей, которые принято называть сайтами. Например, о корпоративной сети с центральным отделением и тремя удалёнными филиалами можно сказать, что они состоят из четырёх сайтов.

Маршрутизатор, с помощью которого сайт клиента подключается к граничному маршрутизатору провайдера PE, называется граничным маршрутизатором клиента CE (Customer Edge router).

На рисунке 16.1 приведён пример VPN A с двумя сайтами, VPN B с тремя сайтами и VPN C с четырьмя сайтами.

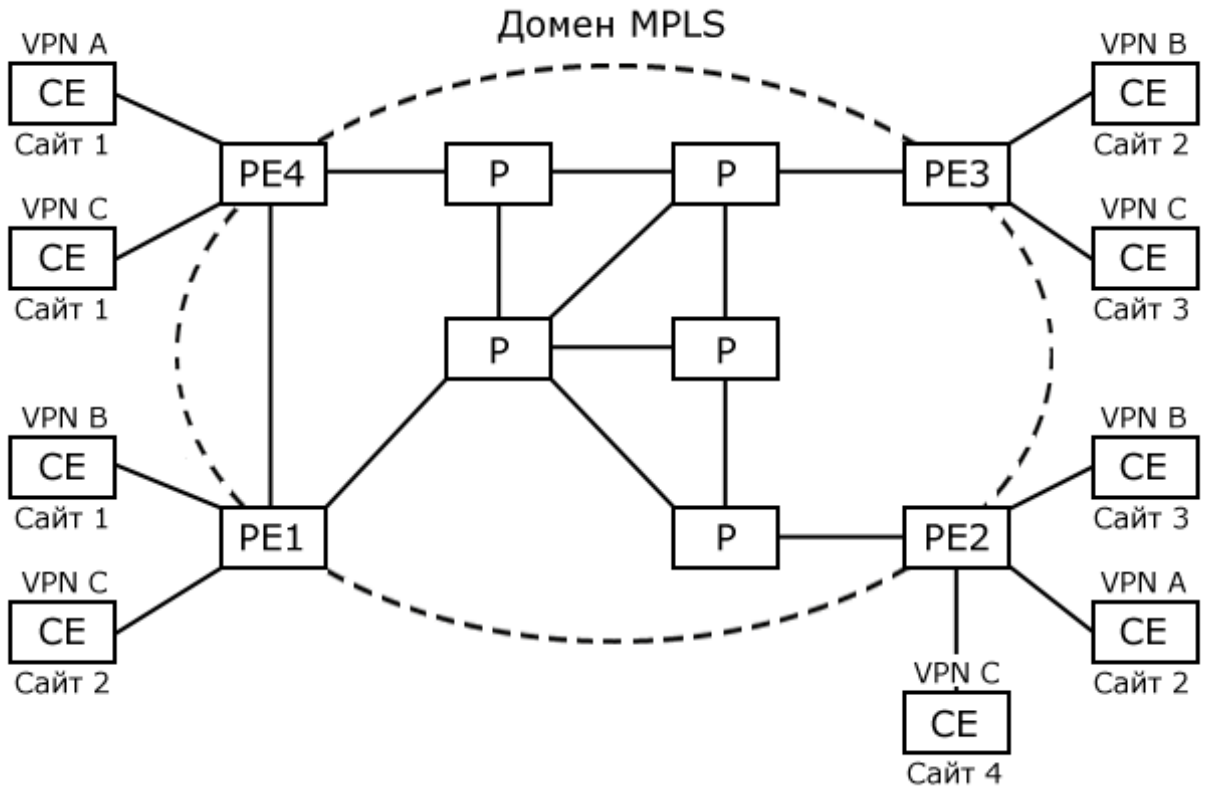


Рис. 16.1. Пример общей модели MPLS L3VPN

16.2.2. Таблицы маршрутизации в VPN

Маршрутизаторы CE и PE связаны обычным физическим каналом по протоколу канального уровня (например, PPP, Ethernet, FR, ATM). Магистральная сеть провайдера MPLS, состоящая из внутренних маршрутизаторов P, обеспечивает продвижение пакета с помощью меток. Граничные маршрутизаторы PE содержат VPN-маршрутизаторы для поддерживаемых сайтов VPN, а внутренние маршрутизаторы P не содержат VPN-маршрутов. На каждом маршрутизаторе PE создается два типа таблиц маршрутизации:

- глобальная таблица маршрутизации создаётся на основе сообщений из магистральной сети MPLS;
- таблица маршрутизации VRF (VPN Routing and Forwarding table) создаётся на основе сообщений маршрутизации, поступающих от граничных маршрутизаторов CE и PE.

На рисунке 16.2 приведена общая схема формирования таблиц маршрутизации VPN в граничном маршрутизаторе.

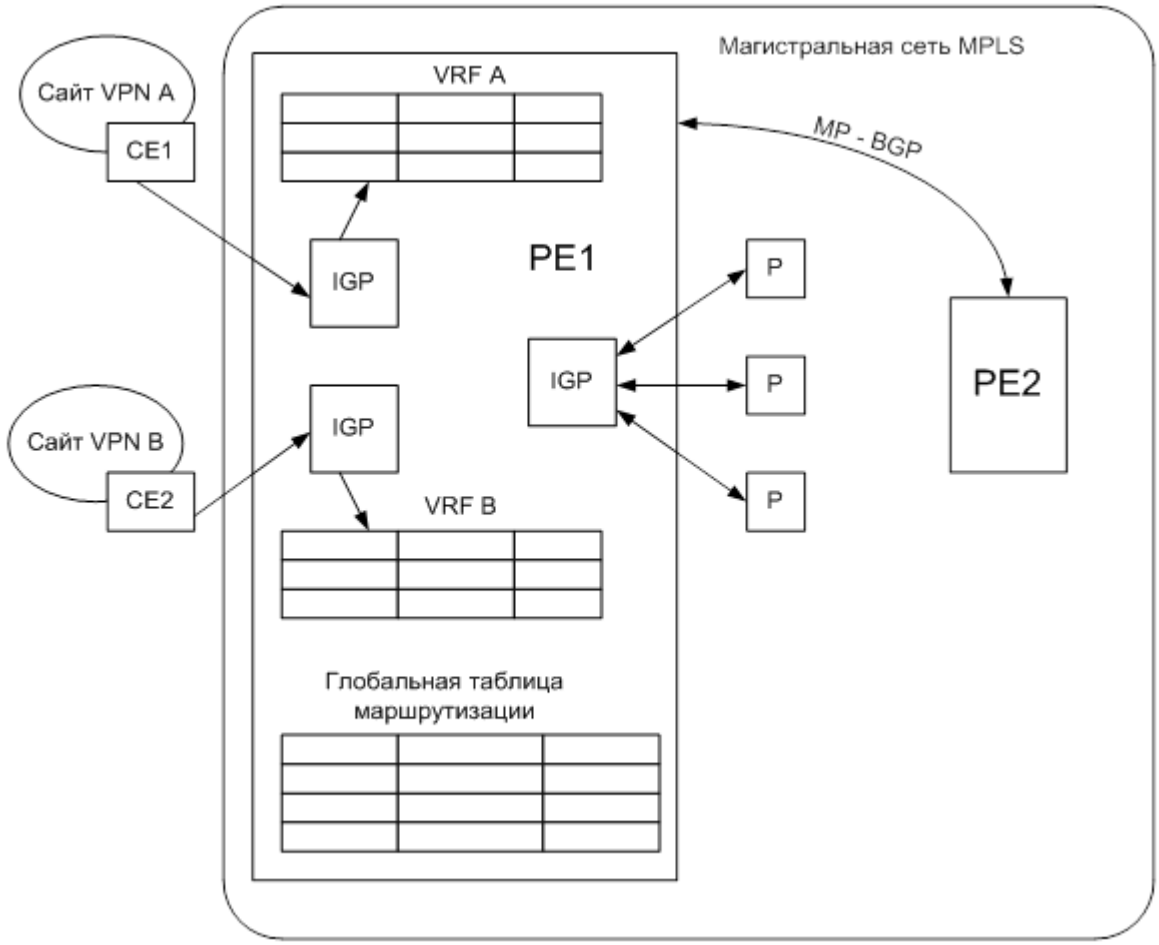


Рис. 16.2. Общая схема формирования таблиц маршрутизации VPN в граничном маршрутизаторе

Для работы VPN с высокой степенью защиты от несанкционированного доступа необходимо, чтобы сведения о маршрутах не становились известными за пределами этих VPN. Глобальная таблица маршрутизации создаётся с помощью внутренних шлюзовых протоколов IGP (Interior Gateway Protocols) IP-сети, к которым относится протокол OSPF. Таблица маршрутизации создаётся этими протоколами на участке между PE и смежными с ним внутренними маршрутизаторами P. Она включает метку для установки в исходящий информационный пакет из выходного маршрутизатора PE во входной маршрутизатор P тракта LSP конкретной VPN. Эта метка устанавливается в исходящем пакете наверху стека. На рисунке 16.2 приведены три смежных с PE1 внутренних маршрутизатора P. Таблица маршрутизации VRF создается протоколами маршрутизации IGP между PE и CE, а также протоколами BGP между граничными маршрутизаторами PE. Как показано на рисунке 16.1, граничный маршрутизатор PE может принадлежать одновременно нескольким VPN. Здесь PE2 принадлежит трём VPN (VPN A, VPN B, VPN C). Каждая таблица VRF в

маршрутизаторе PE содержит необходимые данные маршрутизации для одного сайта (и, соответственно, одного маршрутизатора пользователя CE) одной VPN. Это обеспечивает эффективную изоляцию подсетей и позволяет разным предприятиям использовать перекрывающиеся множества частных IP-адресов. В таблице VRF маршрутизатора PE1 (рис. 16.2), подключенного к двум сайтам разных VPN (VPN A и VPN B), содержатся две таблицы – VRF A и VRF B. Если бы эти два сайта принадлежали одной и той же VPN, то число таблиц VRF также было бы две. В каждой VRF содержатся префикс подсети сайта, соседний CE и другие поля. Адреса подсетей (префиксы) могут совпадать. PE-маршрутизатор преобразует их в уникальные адреса.

16.2.3. Формирование таблицы маршрутизации сообщениями MP-BGP

Помимо указанных в VRF данных маршрутов от подсоединённых сайтов, каждая таблица дополняется маршрутами, получаемыми от других сайтов этой VPN. Механизмом, с помощью которого сайты обмениваются маршрутной информацией, является многопротокольное расширение для протокола BGP (MP-BGP, MultiProtocol extention for BGP). С помощью MP-BGP граничные маршрутизаторы PE обмениваются маршрутной информацией из своих таблиц VRF, при этом дополняя их необходимыми для VPN определёнными значениями. К ним относятся метки, обеспечивающие туннелирование в VPN. При этом сообщения MP-BGP отправляются только тем маршрутизаторам PE, к которым подключены сайты конкретной VPN. Протокол MP-BGP передаёт из PE преобразованный IP-префикс подсети (адрес подсети) в VPN-префикс, добавляя к нему 64 битовый признак маршрута RD (Route Distinguisher). В результате на маршрутизаторе PE все адреса, относящиеся к разным VPN, будут отличаться, даже если они имеют одинаковые префиксы IP-сети. Значения RD задаются администратором сети.

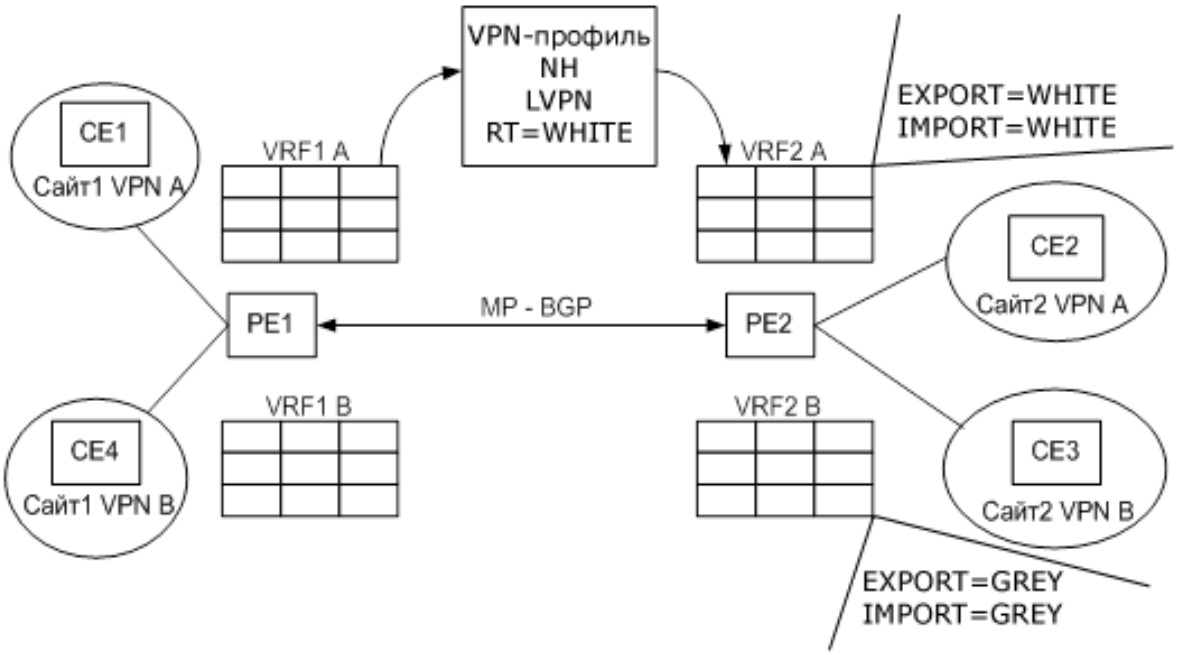


Рис. 16.3. Формирование таблицы маршрутизации сообщениями MP-BGP

На рисунке 16.3 показано формирование таблицы маршрутизации VRF с помощью сообщений протокола MP-BGP. Здесь показана передача сообщений от PE1 в PE2. К каждому из PE подключен сайт, принадлежащий одной и той же VPN A. В состав этих сообщений включены приведенные на рис. 16.3 следующие характеристики.

- Формируется VPN-профиль в PE1 для передачи маршрутизатору PE2, включающий префикс IP-сети сайта 1 VPN A и признак маршрута RD.
- Указывается PE1 и адрес выходного внешнего интерфейса PE1, через который проходит тракт LSP к адресу назначения. При этом назначается метка LVPN, указывающая на таблицу VRF1 A и интерфейс маршрутизатора PE1, к которому подключен сайт 1 VPN A.
- Задаётся расширенный атрибут сообщества – маршрутная цель RT (Rout Target). Этот атрибут идентифицирует набор сайтов (и соответствующих таблиц VRF), входящих в данную VPN A, которые формируют топологию VPN.

Эти сообщения протокол MP-BGP посылает только своим соседям, которые указаны в атрибуте RT. Когда входной маршрутизатор PE2 получает сообщение, он отбрасывает признак маршрута RD, а затем помещает в VRF2 A значение LVPN и префикса IP-сети сайта 1 VPN A. Это показано на рис. 16.4 следующего подраздела.

16.2.4. Пересылка пакетов в VPN

MPLS-протокол LDP обеспечивает получение всеми PE-маршрутизаторами метки, связанные с данным PE-маршрутизатором. Сеть MPLS готова к обмену VPN-пакетами в тот момент, когда входной PE-маршрутизатор получает метку для выходного PE-маршрутизатора. На рис. 16.4 показано перемещение пакета данных между узлами разных сайтов одной VPN. Пересылка на основании метки по магистрали провайдера базируется либо на технологии коммутации по меткам, либо на маршрутах перераспределения потоков. При передаче пакета по магистрали пакет данных пользователя содержит два уровня меток. Верхняя метка направляет пакет к требуемому PE-маршрутизатору, а вторая метка указывает на таблицу VRF, логически связанную с выходным интерфейсом CE-маршрутизатора пункта назначения. Получив IP-пакет через какой-либо интерфейс от CE, PE-маршрутизатор логически связывает его с комплексом VRF, в результате чего создаётся нижняя метка, логически связанная с выходным PE-маршрутизатором (который идентифицирует таблицу VRF адресата маршрута получателя и выходной интерфейс выходного PE-маршрутизатора). Из глобальной таблицы пересылки PE-маршрутизатор получает верхнюю метку, которая указывает PE-маршрутизатор следующего транзитного перехода. PE-маршрутизатор помещает обе метки в стек меток MPLS. Этот стек меток присоединяется к VPN-пакету и направляется к следующему транзитному переходу. P-маршрутизаторы анализируют верхнюю метку и направляют пакет по сети к требуемому узлу. На выходном PE-маршрутизаторе верхняя метка удаляется и исследуется нижняя, указывающая таблицу VRF адресата маршрута и выходной интерфейс. После этого нижняя метка также удаляется, а IP-пакет посылается на требуемый CE-маршрутизатор.

Пусть, например, с сайта 2 VPN A узел с адресом 10.2.1.1/16 отправляет пакет к узлу сайта 1 этой же сети VPN, имеющему адрес 10.1.0.3./16. Стандартными транспортными средствами IP-пакет доставляется на пограничный маршрутизатор сайта CE3, в таблице которого для номера сети 10.1.0.0 в качестве следующего маршрутизатора указан маршрутизатор PE2. На маршрутизатор PE2 пакет поступает с интерфейса 2, поэтому для дальнейшего продвижения пакета он обращается к таблице VRF2 A, связанной с данным интерфейсом. В таблице VRF2 A адресу 10.1.0.0 соответствует запись протокола BGP, которая указывает, что следующим маршрутизатором (NH) для пакета определён маршрутизатор PE1. Поле метки содержит значение LVPN=7, определяющее интерфейс выходного маршрутизатора PE1. Это значение должно быть присвоено пакету для того, чтобы он попал в нужную сеть VPN. Здесь также указывается, что запись была сделана протоколом BGP, а не IGP. На этом

основании маршрутизатор PE2 «понимает», что очередной маршрутизатор не является непосредственным соседом и путь к нему надо искать в глобальной таблице маршрутизации. В глобальной таблице для адреса PE1 указывается начальное значение метки пути LSP, равное 3. Способ прокладки пути между маршрутизаторами PE1 и PE2 описан выше в главе 15.

В сетях MPLS VPN используются иерархические свойства путей MPLS, за счет чего пакет может быть снабжен несколькими метками, помещаемыми в стек. На входе во внутреннюю сеть поставщика, образуемую маршрутизаторами P, пакет будет снабжен двумя метками LVPN=7 и L=3. Метка LVPN интерпретируется как метка нижнего уровня – оставаясь на дне стека, она не используется, пока пакет путешествует по туннелю PE1-PE2. Продвижение пакета происходит на основании метки L верхнего уровня стека. Каждый раз, когда пакет проходит очередной маршрутизатор P вдоль туннеля, метка L анализируется и заменяется новым значением. И только после достижения конечной точки туннеля – маршрутизатора PE1 – из стека извлекается метка LVPN. В зависимости от её значения пакет направляется на тот или иной выходной интерфейс маршрутизатора PE1 (на рис. 16.4 этот интерфейс обозначен Int 7). Из таблицы VRF, извлекается запись о маршруте к узлу назначения, указывающая на CE1 в качестве следующего маршрутизатора. Заметим, что запись об этом маршруте была помещена в таблицу VRF1A протоколом IGP. Последний отрезок путешествия пакета от CE1 до узла 10.1.0.3 осуществляется традиционными средствами IP.

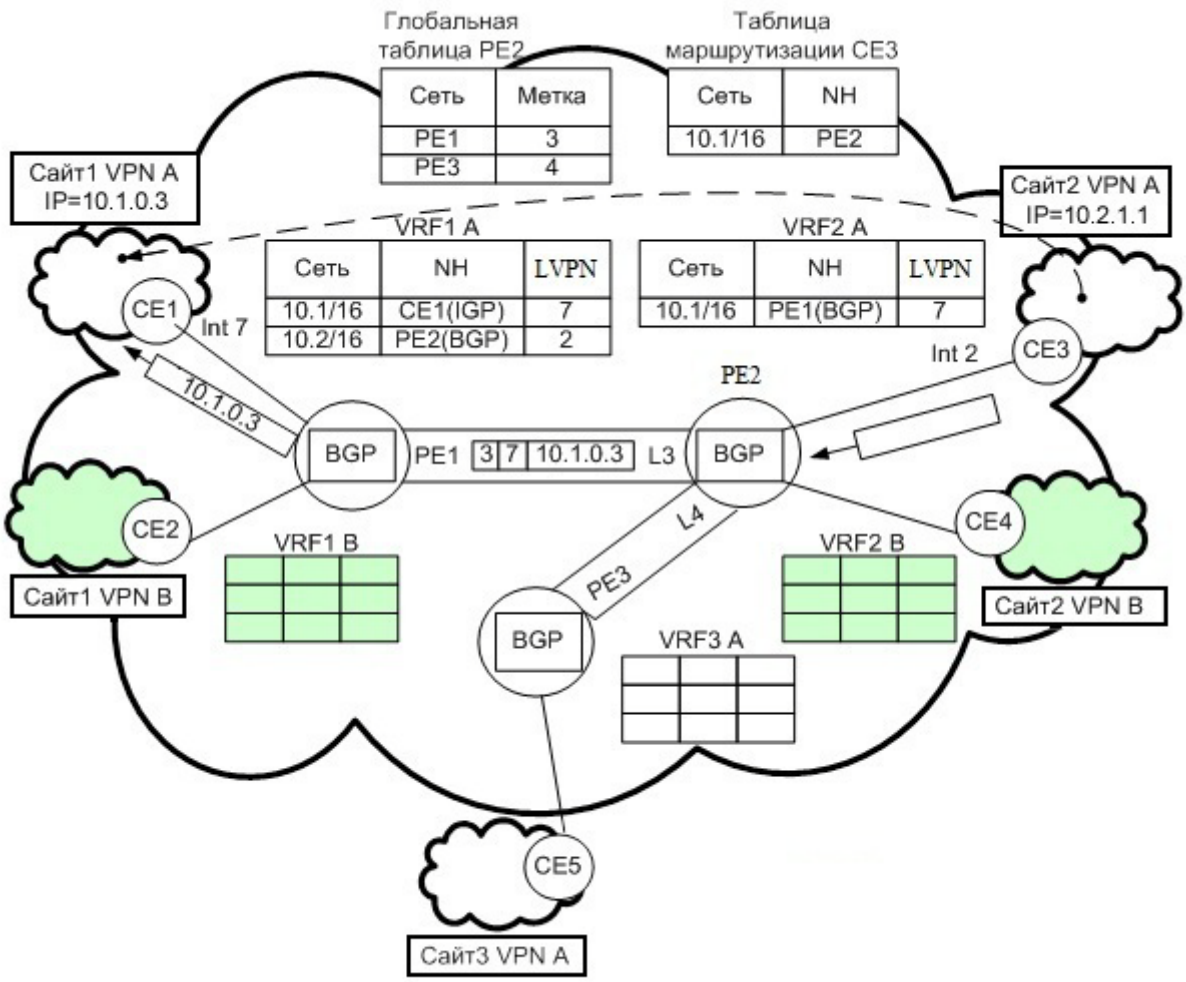


Рис. 16.4. Перемещение пакета данных между узлами VPN
Здесь приняты сокращения:

- NH (next hop) – следующий маршрутизатор;
- VRF1 A, VRF2 A, VRF3 A – таблицы маршрутизации (соответственно в PE1, PE2, PE3) относящиеся к VPN A;
- VRF1 B, VRF2 B – таблицы маршрутизации (соответственно в PE1, PE2), относящиеся к VPN B.

Рассмотрим перенос пакетов двух разных VPN через домен MPLS. Для коммутации IP-пакетов между устройствами PE используются две метки стека. Эти метки назначаются во входном PE IP-пакету, полученному от CE. Одна («внешняя») используется непосредственно для коммутации пакета маршрутизаторами домена MPLS. Внешняя метка определяет путь LSP от одного PE до другого. Вторая метка («внутренняя») идентифицирует VRF на выходном PE, которому принадлежит IP-пакет.

Рассмотрим домен MPLS, к которому подключены два VPN - VPN A и VPN B (рис. 16.5). VPN A образован сайтами, включающими CE1 и CE2, а VPN B - CE3 и CE4. Как видно из рисунка, совпадают префиксы IP-адреса узлов CE1, CE3 (10.1.1.0/24), а также префиксы IP-адреса узлов CE2, CE4 (10.2.1.0/24).

На рисунке показано прохождение двух пакетов через домен MPLS.

На рисунке приняты следующие обозначения:

(1.1) – содержание полей IP-пакета, поступившего из CE1 на PE1. Поле d означает IP-адрес пользователя-получателя, а поле s IP-адрес пользователя-отправителя.

(1.5) – содержание полей IP-пакета, поступившего из PE2 в CE2.

Аналогичные содержания полей IP-пакета VPN B (от CE3 до CE4). IP-адреса пакетов обеих VPN совпадают.

Рис. 16.5. Схема прохождения пакетов VPN через домен MPLS

Обозначения (1.2), (1.3), (1.4) включают состав полей пакетов VPN A, поступающих на маршрутизаторы P1, P2, PE2. Аналогично обозначения (2.1), (2.2), (2.3) включают состав полей пакетов VPN B, поступающих на эти же маршрутизаторы. В PE1 устанавливается внешняя метка, равная 345. Эта метка позволяет создать LSP-туннель от PE1 до PE2. Верхняя метка в пакетах VPN позволяет произвести коммутацию в P1 (смену метки 345 на 600). Поскольку P2 является предпоследним маршрутизатором LSP-туннеля, в нем производится удаление верхней метки. В результате в пакетах VPN в маршрутизаторе PE2 содержатся «внутренние» метки (соответственно для пакета VPN A – 1000, для пакета VPN B – 1020). Эти метки идентифицируют пакет на PE2 и указывают конкретный интерфейс к

пользователю – Int1 для IP-пакета VPN A и Int2 для IP-пакета VPN B.

Рассмотрим прохождение пакета из VPN A от CE1 до CE2 через домен MPLS:

- PE1 получает пакет от CE1. По интерфейсу, от которого пришел пакет PE1 определяет, что пришедший пакет принадлежит VRF A.
- По VRF-таблице PE1 определяет, что подсеть 10.2.1.0/24 (которой предназначен пакет) доступна через домен MPLS и пакету необходимо назначить две метки 1000/345. Метки назначаются и пакет пересылается устройству P1.
- Устройства P1 и P2 на основании своих таблиц коммутации переправляют пакет устройству PE2. Эти таблицы коммутации содержат множества меток и для каждой из них привязку «FEC-метка», что позволяет поддержать заданное качество обслуживания. При этом может быть использована процедура управления трафиком - инжиниринг трафика. Отметим то, что «внешняя» метка 345, назначенная пакету устройством PE1, определяет LSP от PE1 до PE2.
- PE2 получает пакет только с «внутренней» меткой 1000 и на основании таблицы коммутации определяет выходной интерфейс, через который должен быть переслан пакет (уже без метки).

Прохождения пакета из VPN B от CE3 до CE4 через домен MPLS происходит аналогично предыдущему примеру. Отличие лишь в значении «внутренней» метки, которая определяет или другой исходящий интерфейс на PE2 или другой VRF.

Прохождение пакета в обратную сторону, например от CE2 до CE1 происходит также аналогично приведенному примеру, за исключением значений меток. «Внешняя» метка в этом случае будет определять LSP от PE2 до PE1, а «внутренняя» метка будет назначаться устройством PE1 и обозначать VRF или интерфейсы на устройства PE1.

Из рассмотренного примера видно, что один и тот же IP-адрес может использоваться в разных VPN, то есть любая VPN может иметь собственное пространство. Для однозначной идентификации адреса пользователя (даже в том случае, когда узел пользователя использует незарегистрированный частный IP-адрес) было специфицировано семейство адресов VPN-IPv4 Adress Family. Адрес VPN-IPv4 имеет длину 12 байтов, первые восемь из которых занимает префикс, называемый различителем маршрутов RD (Route Distinguisher), а оставшиеся 4 байта содержат IPv4 адрес. Таким образом, решается задача определения разных маршрутов к устройствам, имеющим один и тот же IP-адрес, но принадлежащий разным VPN.

16.2.5. Формирование топологии VPN

При конфигурировании каждой таблицы VRF задаются два атрибута маршрутной цели RT: один для определения политики экспорта, а другой для определения импорта маршрутов. Сравнение значений атрибутов RT в маршрутном сообщении и в параметрах VRF позволяет решить вопрос о принятии или отклонении предлагаемого маршрута, что позволяет формировать топологию сети VPN.

Пусть изображенный на рисунке 16.3 маршрутизатор PE2 получил сообщение от PE1. PE2 проверяет значение атрибута RT (политика экспорта-WHITE) в этом сообщении на совпадение с политикой импорта всех своих таблиц VRF (VRF2 A и VRF2 B). Атрибут RT WHITE совпадает с таблицей импорта VRF2 A, но не совпадает с таблицей импорта VRF2 B (GREY). Поэтому пакеты сайта 1 VPN A будут приниматься только клиентами сайта 2 VPN A и не приниматься клиентами сайта 2 VPN B. Такая топология, когда значения политики экспорта и импорта определенной VPN (на примере рис. 16.4 VPN A) одни и те же, называется полносвязной, то есть каждый сайт может посылать пакеты непосредственно тому сайту, в котором находится сеть назначения.

Существуют и другие варианты топологий VPN. Например, можно создать топологию звезда, когда все сайты общаются друг с другом только через центральный сайт. Для этого политика импорта центрального сайта должна совпадать только с политикой экспорта остальных сайтов, а политика экспорта центрального сайта совпадать с политикой импорта остальных сайтов.

16.2.6. Сравнение VPN-технологий

Настоящий раздел посвящён сравнению VPN-сетей, построенных на технологиях сетей – ATM (VPN- ATM); IP(VPN-IP); MPLS (L3VPN-MPLS). В таблице 16.1 приведено сравнение этих VPN по следующим показателям: уровень сложности при установке и управлении, уровень безопасности, масштабируемость, QoS, стоимость установки. Здесь же приведено пояснение (комментарии) по этим показателям.

Таблица 16.1. Сравнение VPN-технологий

Показатель	**Комментарий**	**VPN-ATM**	**VPN- IP**	**L3VPN-MPLS**

Уровень сложности при установке и управлении	Возможности мониторинга и анализа потоков данных для быстрого создания новых служб, повышения уровня ИБ, QoS и SLA.	Низкий	Средний	Высокий
Уровень ИБ	Возможности обеспечивать различные уровни ИБ, включая аутентификацию, шифрование.	Высокий	Высокий	Высокий
Масштабируе-мость	Возможности расширения служб VPN малых и средних предприятий до сетей крупных предприятий.	Средняя	Средняя	Высокая
Качество обслуживания	Возможности обеспечивать требования пользователей к показателям QoS.	Высокое	Никакое	Высокое
Стоимость установки VPN	Прямые и косвенные расходы на установку VPN.	Высокая	Средняя	Низкая

Приведём более подробно следующие преимущества VPN-сетей MPLS в части:

- обеспечения качества обслуживания;
- масштабируемости;
- информационной безопасности;
- гибкости создания сети;
- гибкости адресации;
- объединения различных типов данных;
- инжиниринг трафика (перераспределение потоков);
- сложности проектирования.

Обеспечение качества обслуживания

Механизмы MPLS-VPN обеспечивают пользователям необходимое качество соединения на

всем протяжении маршрута, а провайдерам позволяют гарантировать выполнение условий соглашения об уровне обслуживания (SLA).

Технология MPLS реализует модель дифференцированного обслуживания DiffServ, позволяющая обеспечить QoS путем разделения трафика соединений на небольшое число классов. Каждому классу предусмотрено назначение приоритета обслуживания блоков данных. Выделение сетевых ресурсов производится для каждого такого класса, а не каждого соединения, как в сети ATM, по определённому набору требуемых пользователями показателей качества и трафика.

Масштабируемость

Использование технологии MPLS позволяет создавать в одной и той же сети десятки тысяч VPN-структур. MPLS не требуют установления соединения «точка-точка» для создания VPN-сетей. Сайт пользователя имеет одноранговую связь только с одним граничным маршрутизатором PE, а не со всеми маршрутизаторами CE, которые принадлежат к VPN-сети.

Информационная безопасность

VPN-сети MPLS обеспечивают такой же уровень защиты от несанкционированного доступа, как и VPN-сети ATM. Следует отметить, что MPLS-VPN не обеспечивает целостность и конфиденциальность передаваемых данных в отличие от VPN на базе IPSec. В случае необходимости технология MPLS-VPN допускает применение IPSec для обеспечения мер информационной безопасности. Пакеты одной VPN не могут попасть в другую VPN. Безопасность обеспечивается на границе инфраструктуры провайдера, где пакеты пользователя направляются в каждую VPN. Получить доступ к граничному маршрутизатору практически невозможно, поскольку IP-пакеты однозначно идентифицируются по меткам.

Гибкость создания сети

При построении узел пользователя может находится в нескольких VPN, что предоставляет максимальную гибкость при построении инфраструктуры. Функция MPLS выполняется в сети провайдера, а в конфигурировании оборудования пользователем либо вообще нет необходимости, либо требуется лишь незначительное. Среда MPLS прозрачна для маршрутизаторов CPE, т.е. CPE–устройствам пользователя установка MPLS не требуется.

Гибкая адресация

Пользователи используют собственные адресные пространства и не требуется преобразования открытых IP-адресов.

Объединение различных типов данных

Объединение в одном потоке различных типов данных, речи и видео.

Инжиниринг трафика

Технология MPLS позволяет перераспределять потоки, перемещая нагрузку с чрезмерно используемых частей сети в неполностью используемые. Маршрутизация с перераспределением потоков и резервированием ресурсов позволяет провайдерам в максимальной степени использовать сетевые ресурсы, обеспечить высокое качество обслуживания QoS и добиться оптимальной работы сети. Маршрутизация в MPLS позволяет оператору применять явно заданные маршруты и принудительно направлять по ним потоки данных, что заменяет традиционные методы IP-маршрутизации и предоставляет пользователю быстрое восстановление работы сети в случае отказа канала связи или устройств. При этом достигается оптимизация недостаточно загруженных каналов и более эффективная маршрутизация.

Сложность проектирования

Недостатком VPN на базе ATM является необходимость создания большого числа постоянных виртуальных каналов (число сочетаний числа сайтов по два). При этом сохраняется некоторая часть ручного труда и вероятность ошибочных действий администрации.

ГЛАВА 17. Цифровая сеть с интеграцией служб. Общеканальная сигнализация ОКС№7

В настоящее время на сетях связи общего пользования единой сети электросвязи России, как и во многих других развитых странах мира, в эксплуатации находятся:

- телефонные сети связи общего пользования ТфОП, построенные на базе технологии цифровых сетей связи с интеграцией служб ЦСИС (ISDN, Integrated Services Digital Network). Такие сети часто называют сетями ТфОП/ISDN;
- сотовые сети подвижной связи стандарта GSM (Global System Mobile);
- интеллектуальные сети IN (Intelligent Network).

Для реализации соответствующих услуг в этих сетях необходимо обеспечить передачу сигнальных и служебных сообщений между узлами сети. Для этих целей используется в составе оборудования общеканальная система сигнализации №7 (ОКС-7 или ОКС№7). В технической литературе ОКС№7 иногда называют системой сигнализации №7 (SS7, Signaling System №7). Настоящая глава посвящена технологии ISDN, включающая ОКС№7 [33].

17.1. Цифровая сеть с интеграцией служб ISDN

17.1.1. Структура сети ISDN

Цифровая сеть с интеграцией служб ЦСИС (ISDN, Integrated Services Digital Network) позволяет предоставлять пользователям как телефонию, так и передачу данных. Однако доля абонентов ISDN, пользующихся передачей данных, в настоящее время составляет несколько процентов от общего числа абонентов, пользующихся только телефонией. Тем не менее, изложение этого материала вызвано не только тем, что ISDN действует в существующих ТфОП, но и другими техническими причинами. В первую очередь это относится к используемой в этой сети системы сигнализации ОКС№7. Согласно определению в рекомендации ITU-T Q.9 [34] под ***сигнализацией*** понимается обмен неречевой информацией, которая регулирует процесс установления, разрыва и управления вызовом, а

также управление сетью в автоматизированном телекоммуникационном оборудовании. Нижние три уровня ОКС№7, соответствующие модели OSI, используют не только при обслуживании телефонной службы фиксированной сети ТфОП, мультимедийных служб абонентов ISDN, но и в таких современных технологиях, как сотовые сети подвижной связи и интеллектуальные сети.

Цифровую сеть с интеграцией служб ISDN России можно рассматривать как этап развития телефонной сети общего пользования ТфОП. Все региональные и местные операторы связи РФ, подключенные к сети ТфОП/ISDN оператора ОАО «Ростелеком» (междугородной и международной связи на сети общего пользования) имеют постоянный доступ к таким сетям всего мира. В качестве терминального оборудования в предельном случае абонент, пользующийся телефонией и передачей данных ISDN, может иметь до 8 различных устройств (телефон, компьютер, телефакс, телефон с возможностью передачи изображений и т.д.). На рисунке 17.1 приведен принцип иерархии ОКС№7 телефонной сети общего пользования России. На рисунке показаны узлы коммутации сети ТфОП России (АТС, УИВС, АМТС, УАК, МЦК). Узлы коммутации сети включают следующие пункты сигнализации ОКС№7:

- оконечный пункт сигнализации SEP (Signaling End Point), включенный в оборудование АТС;
- промежуточный пункт сигнализации SP (Signaling Point), обеспечивающий связный режим сигнализации;
- транзитный пункт сигнализации STP (Signaling Transfer Point), передающий сообщения в квазисвязанном режиме сигнализации;
- пункт сигнализации SPR (Signaling Relay Point), с функцией переприема сообщений SCCP.

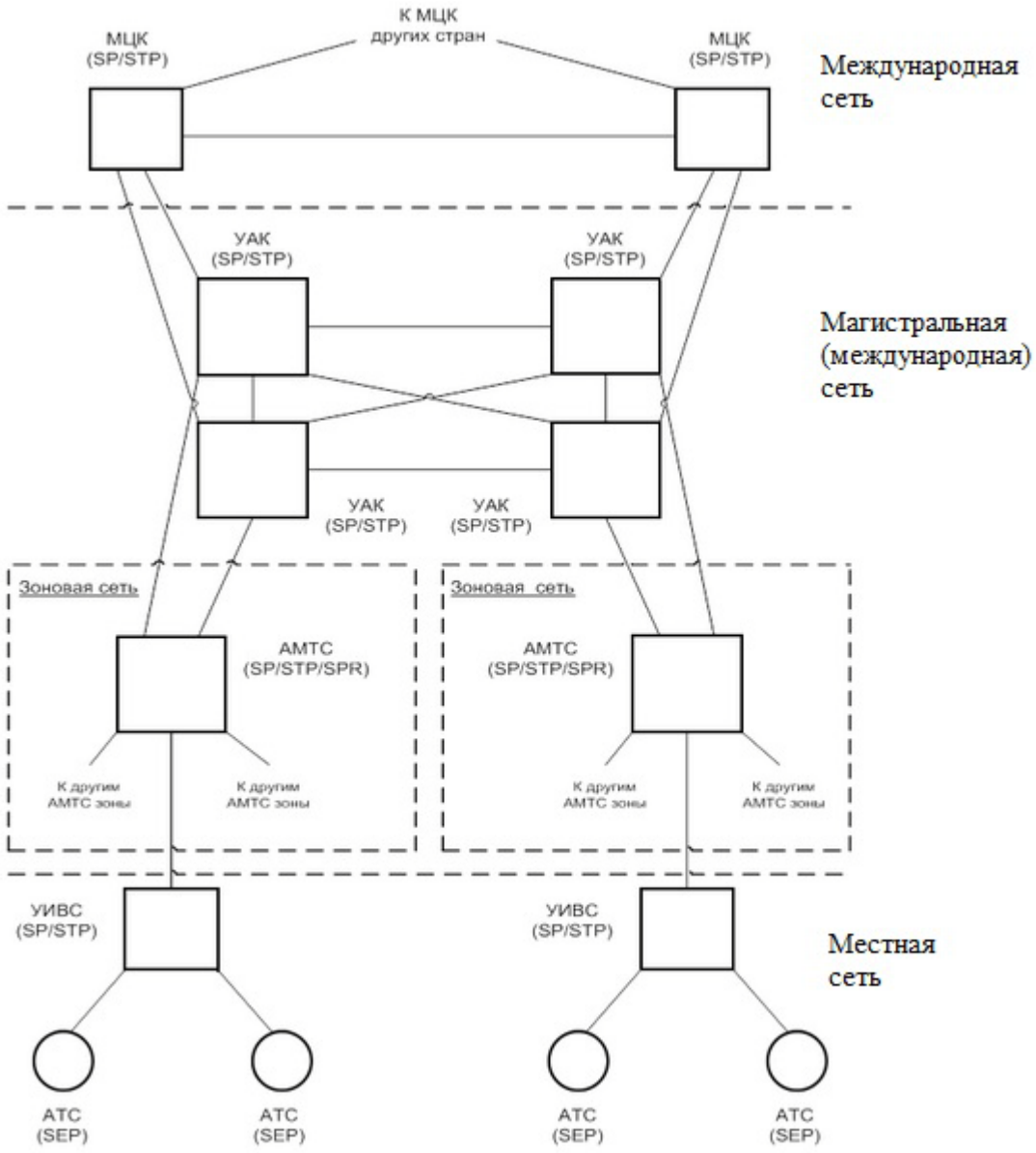


Рис. 17.1. Принцип иерархии ТфОП в России

На рис. 17.1 в скобках приведены пункты сигнализации, входящие в узлы коммутации ТфОП. Сеть ТфОП вместе с пунктами сигнализации ОКС№7 составляет следующие уровни иерархии (снизу вверх):

- местная сеть;
- зоновая сеть междугородной сети;
- магистральная сеть междугородной сети;

- международная сеть.

Не во всех местных и зоновых сетях имеет место иерархическое построение. На этом рисунке не приводятся полные конфигурации уровней из-за их многообразия. Телефонная сеть общего пользования ЕСЭ России на крупных местных сетях строится по двухуровневому принципу иерархии с использованием узла исходящих и входящих сообщения (УИВС). Территория московской городской телефонной сети разбита на восемь миллионных районов. В каждом из этих районов организуется узел входящего сообщения (УВС) и узел исходящего сообщения (УИС). На УИС поступают сообщения абонентов этого района. УИС соединяется со всеми УВС других районов. УИС и УВС соединяются в такой сети с автоматической междугородней станцией АМТС. АМТС образует двухуровневую сеть. Нижний уровень представляет зоновую междугородную сеть, образуемую в пределах территории одного или нескольких субъектов Российской Федерации (регионов). Верхний уровень представляет магистральную междугородную сеть узлов автоматической коммутации, обеспечивающих транзит потоков сообщений между зоновыми сетями. Уровень международной сети образуют международные центры коммутации МЦК, подключенные к сетям связи общего пользования иностранных государств.

На рис. 17.2 приведена структура сети ISDN. Сеть ISDN состоит из абонентского доступа и транспортной сети. Международным союзом электросвязи – сектор стандартизации телекоммуникаций МСЭ-Т разработан протокол цифровой абонентской сигнализации №1. Этот протокол DSS-1 (Digital Subscriber Signalling 1, цифровая абонентская сигнализация) между пользователем ISDN и сетью ориентирован на передачу сигнальных сообщений через интерфейс «пользователь-сеть» по D-каналу этого интерфейса. В ISDN определено два режима:

- Режим, использующий канал сигнализации D со скоростью 16 кбит/с, который управляет двумя информационными каналами B=64 кбит/с. Этот режим называется базовым BRI (Basic Rate Interface, интерфейс основной скорости) и используется для подключения терминалов. Каждый B-канал является «собственностью» этого пользовательского терминала.
- Режим, использующий канал сигнализации D со скоростью 64 кбит/с, который управляет 30-тью информационными каналами B, работающими также со скоростью 64 кбит/с. Этот режим называется первичным PRI (Primary Rate Interface, интерфейс первичной скорости).

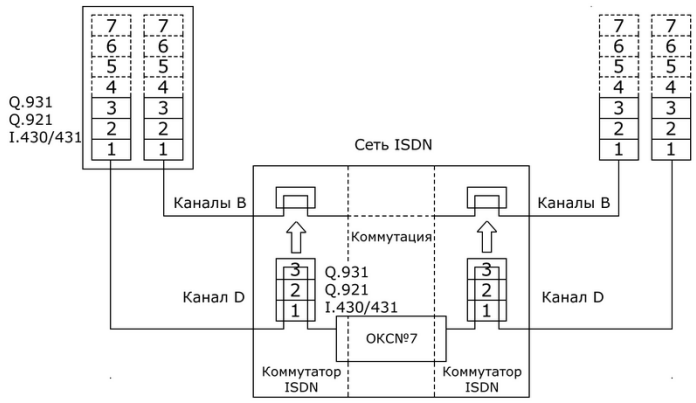


Рис. 17.2. Структура сети ISDN

Протоколы DSS1 включают рекомендации ITU-T трех нижних уровней – I.430/I.431, Q.921, Q.931. Для абонентского доступа и системы ОКС№7 ISDN характерна общая концепция централизованной сигнализации. В отличие от X.25, где сигнализация осуществляется по тем же каналам, по которым передается информация, сигнализация в ISDN осуществляется по отдельным каналам. Технологии сигнализации на абонентском доступе и в транспортной сети отличаются. В первом случае используется один канал сигнализации (D), а во втором сеть каналов сигнализации (система ОКС№7).

17.1.2. Абонентский доступ сети ISDN

17.1.2.1. Функции физического и канального уровней

Рассмотрим функции уровней стека протоколов DSS-1. Физический уровень по протоколу ITU-T I.430 [35] выполняет функцию формирования каналов B и D. В случае базового режима происходит дуплексная передача со скоростью 192 бит/с, что обеспечивается временным мультиплексированием двух B-каналов по 64 кбит/с и одного D-канала 16 кбит/с, а также 48 кбит/с для синхронизации и техобслуживания. Цикл 250 мксек (4000 циклов в секунду) включает 48 бит:

- для каждого канала B по 2 байта. Канал B является информационным для передачи по нему речи или данных. Он предоставляется пользователям в режиме коммутации канала;
- для канала сигнализации D - 4 бита. Он использует коммутацию пакетов;

- для канала синхронизации -12 бит.

В результате скорости каналов B1=B2=16 бит/250 мксек=64 кбит/с, D=4 бит/250 мксек=16 кбит/с. Общая скорость передачи данных информации и сигнализации составляет 144 кбит/с. Канальный уровень, определенный в рекомендациях ITU-T Q.920 [36] и Q.921 [37] принадлежит к семейству протоколов HDLC (High-level Data Link Control). К этому же семейству принадлежит и протокол LAP-B, который используется на канальном уровне сети передачи данных стандарта X.25. Протокол LAP-D также управляет потоком кадров, как и протокол LAP-B, но имеет некоторые отличия в адресном поле. В частности, это относится к методу идентификации терминального оборудования (автоматический или неавтоматический). Эти отличия LAP-B от LAP-D несущественны с точки зрения описания ISDN, а поэтому не подлежат подробному рассмотрению в настоящем материале. Основная задача LAP-D состоит в безошибочном переносе сообщений третьего уровня.

17.1.2.2. Функции сетевого уровня

Сетевой уровень, определенный в рекомендациях ITU-T Q.931 [38], содержит функции, обеспечивающие установление, сопровождение и разъединение соединений, предоставленных сетью пользователям ISDN в режиме коммутации каналов. Обмен необходимой для этого сигнальной информацией между функциями уровня 3, размещенной в оборудовании пользователя и в оборудовании сети, осуществляется через интерфейс «пользователь-сеть» с помощью сообщений сетевого уровня. Любое сообщение уровня 3 DSS-1 содержит три элемента: дискриминатор протокола, метку соединения и тип сообщения. Одной из функций дискриминатора протокола является – различить сообщения ISDN от сообщений, используемых в других сетях, использующих протокол Q.931, таких как Frame Relay. Метка соединения (CR-call reference) является целым числом, используемым для идентификации коммутируемой связи, к которой относится сообщение. Значение метки уникально на той стороне интерфейса, которая явилась инициатором этой связи, и только внутри одного логического соединения уровня 2. Метка присваивается на время обслуживания конкретного вызова, и после окончания его обслуживания может быть использована для идентификации других соединений. Если вызов поступает от сети, то метку соединения назначает входящая АТС.

Третий информационный элемент - тип сообщения образует несколько категорий:

- сообщения, используемые в процедуре фазы установления соединения. Таково, например, сообщение SETUP (запрос соединения или запрос вызова), которое

посылается пользователем к АТС (или АТС к пользователю) в качестве запроса соединения;

- сообщения, передаваемые в фазе установленного соединения. Таково, например, сообщение USER INFORMATION, которое может быть отправлено во время разговора/передачи данных для пересылки информации «пользователь-пользователь»;
- сообщения фазы разъединения. Таково, например, сообщение DISCONNECT, которое посылается пользователем к сети АТС (или АТС к пользователю), чтобы инициировать процедуру освобождения ресурсов, занятых соединением.

Приведем некоторые информационные элементы, которые являются обязательными для определенных типов сообщений. Отметим в качестве такого обязательного для сообщения SETUP элемента – номер вызываемого и вызывающего абонента, в формат которого входят такие поля как:

- тип номера (международный, междугородний, местный);
- план нумерации, соответствующий рекомендациям ITU-T E.164 и используемый на ТфОП РФ. Могут использоваться и другие планы нумерации такие, как X.121 для сетей передачи данных;
- цифры номера вызываемого и вызывающего абонента.

В качестве информационного элемента «средства доставки информации» содержат требования к этим средствам:

- вид информации: речь, передача данных;
- стандарт кодирования, алгоритм кодирования.

На рис. 17.3 показана диаграмма установления соединения телефонной связи с коммутацией каналов в сети ISDN. На вызываемой стороне у пользователя Б подключено два телефонных аппарата (х и у), которые не заняты во время вызова со стороны А. Оконечные устройства пользователя А и пользователя Б подключены через абонентский доступ DSS-1 к ISDN соответственно через $АТС_А$ и $АТС_Б$.

Приведем описание процесса передачи сигнальных сообщений при установлении телефонного соединения.

1) Абонент А снимает телефонную трубку и набирает номер вызываемого абонента. В АТС передается сообщение SETUP (запрос вызова) с номером вызываемого абонента Б, видом

информации (речь, данные) и другими информационными элементами.

1`) Сообщение SETUP через сеть системы сигнализации ОКС№7 поступает на $АТС_Б$ и далее на вызываемые оконечные устройства х и у пользователя Б.

2), 2`) Оконечное устройство х первым передает вызывающему абоненту через сеть сообщение CALL PROCEEDING (продолжение обслуживания вызова).

3), 4) Все оконечные устройства абонента Б, совместимые с запрашиваемой службой (т.е. х и у) извещает $АТС_Б$ об их готовности к установлению соединения с абонентом А (сообщение ALLERTING). $АТС_Б$ отправляет одно из этих сообщений в сеть (3’).

5), 5`) Вызываемое оконечное устройство х первым передает сообщение CONNECT (соединить), что соответствует тому, что «трубка снята».

6), 6`) Сообщение CONNECT ACK (подтверждение соединения), извещает о подключении соединения между вызывающим оконечным устройством и вызываемым оконечным устройством х.

7), 8) Остальные оконечные устройства вызываемого абонента Б отключаются с помощью сообщения RELEASE (освободить) и подтверждения этого сообщения RELEASE COMPLETE (закончить освобождение).

Если соединение нельзя установить, то устройство вызывающего пользователя извещается об этом с указанием причины.

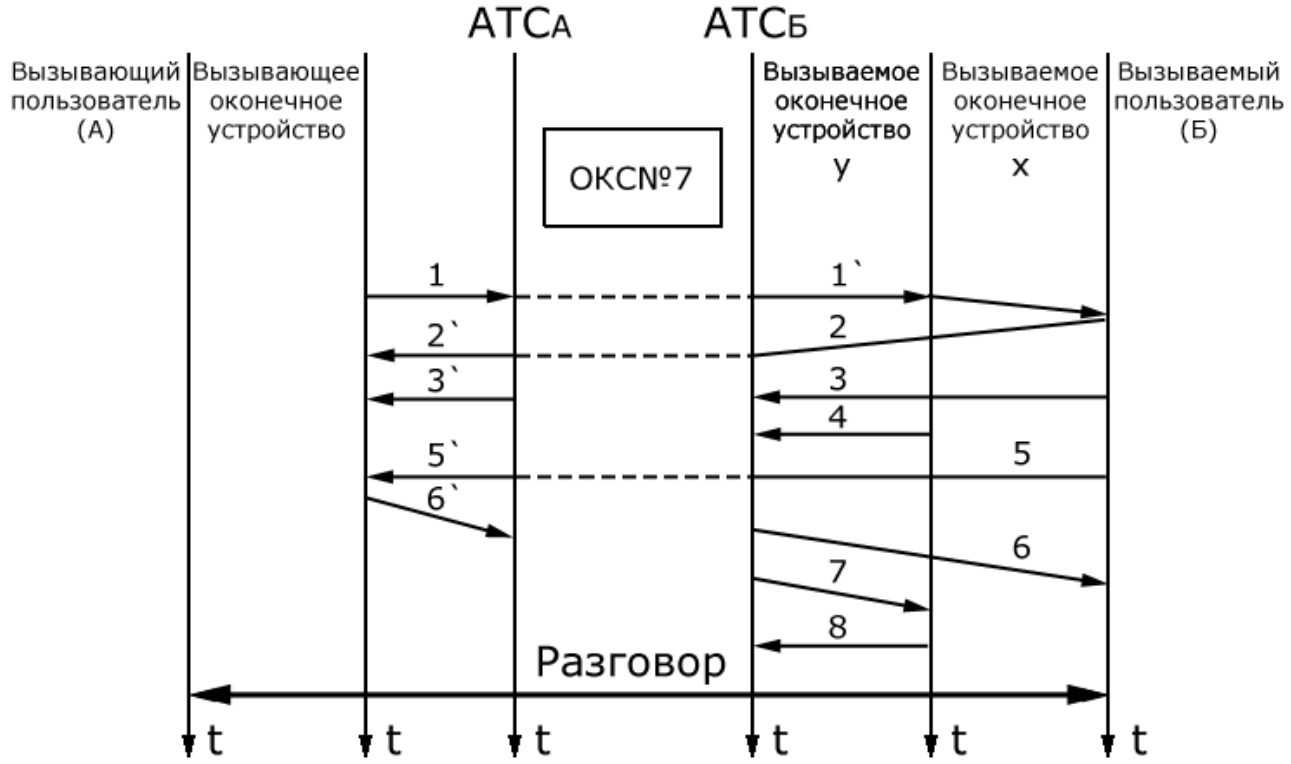


Рис. 17.3. Диаграмма установления соединения телефонной связи с коммутацией каналов в сети ISDN

17.2. Общеканальная сигнализация ОКС№7

В сети ISDN функцию коммутации выполняет система общеканальной сигнализации №7. В литературе эта система также называется ОКС№7 или SS7 (Signaling System 7). ОКС№7 в качестве системы сигнализации управляет установлением и разъединением соединения в ISDN, которая рассматривается как часть и этап развития телефонной сети общего пользования ТфОП. Абонентом ISDN может стать любой абонент ТфОП, имеющий доступ к цифровой АТС с функциями ISDN и соответствующее терминальное оборудование. ОКС№7 является системой с коммутацией пакетов и поэтому по сравнению с коммутацией каналов за счет мультиплексирования более экономично использует каналы связи.

17.2.1. Принцип работы ОКС№7 в сети ТфОП/ISDN

В основе ОКС№7 лежит принцип отделения системы сигнализации ТфОП/ ISDN от системы информационных каналов на уровне построения сети. Это означает, что сеть системы сигнализации ОКС№7 не обязательно совпадает с сетью ТфОП/ ISDN. Это показано на рис. 17.4.

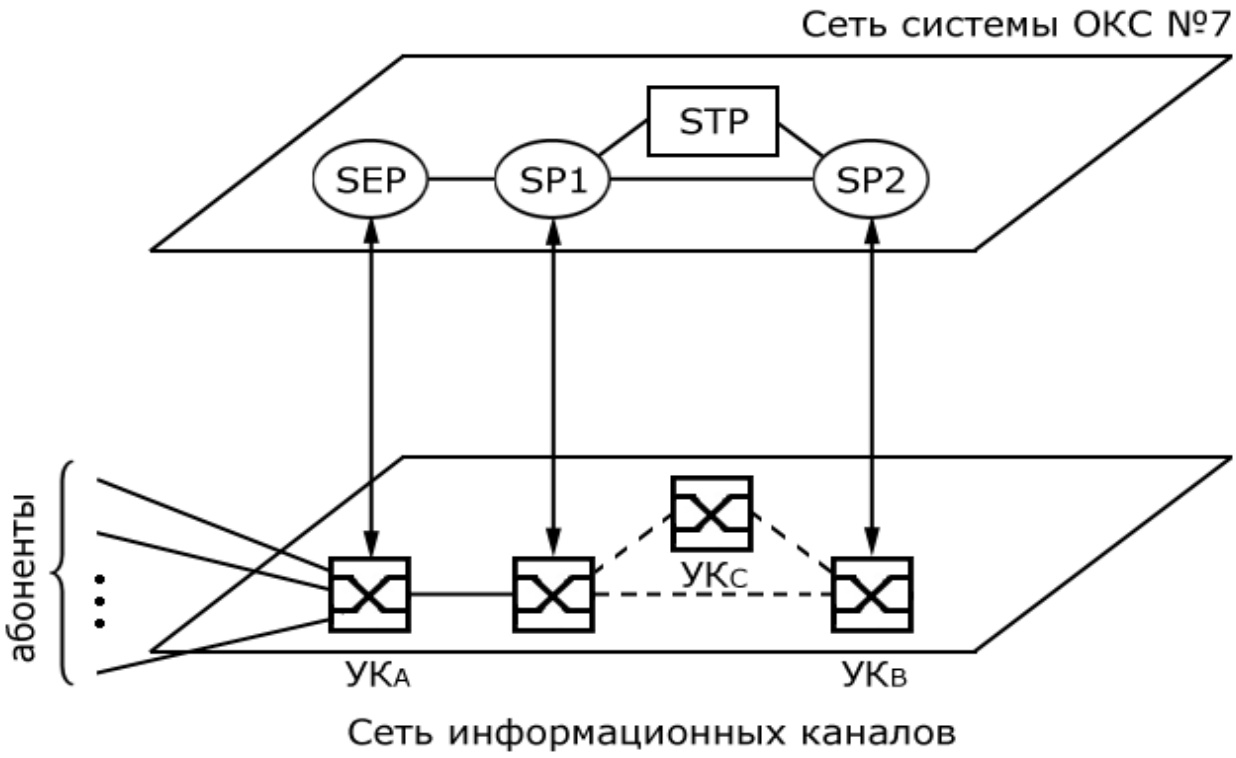


Рис. 17.4. Разделение сети информационных каналов и сети системы ОКС№7

На рисунке приведены пункты сигнализации SEP, SP и STP, входящие в сеть системы ОКС№7.

Пункт сигнализации SP (Signaling Point) является составной частью узла коммутации сети информационных каналов (например, АТС, АМТС и др.) и включает подсистему передачи сообщений (транспортная сеть) и подсистему пользователей сети с интеграцией служб ISUP (Integrated Service User Part). Подсистема ISUP выполняет функции установления коммутируемого соединения информационных каналов. На рис. 17.4 два SP (SP1 и SP2), входящие в узлы коммутации УКА и УКВ определяют свободный информационный канал 64кбит/с. Использование этого канала для установления соединения производится с помощью узлов коммутации.

Пункт сигнализации SP часто называют промежуточным, поскольку он не входит в узлы коммутации ТфОП, к которым подключены непосредственно абоненты сети. Такие пункты сигнализации называются оконечными SEP (Signaling end Point).

В противоположность SP транзитный пункт сигнализации STP (Signaling Transfer Point) выполняет только транспортные функции, т.е. просто транслирует поступающие сообщения сигнализации дальше к SP1 или SP2. В STP отсутствует подсистема пользователя (на рис. 17.4 не показано, в какой узел коммутации он входит). Заметим, что STP может быть

реализовано также на базе выделенного оборудования. На практике на одном и том же узле коммутации функции SP и STP могут быть в различных комбинациях. Пункт сигнализации SP, который генерирует сигнальное сообщение, называется исходящим пунктом сигнализации OP (Originating Point). Пункт сигнализации, которому предназначено сообщение, называется пунктом назначения DP (Destination Point). Различают два режима сигнализации: связанный режим (Associated Mode) и квазисвязанный (Quasi- Associated Mode).

Приведенный на рис. 17.4 случай сигнализации по маршруту SP-SP называется связанным, а по маршруту SP-STP-SP квазисвязанным режимом сигнализации. При квазисвязанном режиме сигнальные сообщения могут передаваться через один или несколько STP. Квазисвязанный режим устанавливает путь, по которому информация проходит через сеть. Этот путь назначается заранее и является фиксированным на заданный период времени. ОКС№7 – это такая система сигнализации, при которой информация управления установлением соединения для всех разговорных каналов и/или каналов передачи данных передается в виде сигнальных сообщений (блоков данных) по одному общему каналу сигнализации. Этот канал может быть организован в любой временном интервале трактов ИКМ, входящем в пучок соединяющих две взаимодействующие АТС (рис. 17.5).

Рис. 17.5. Принцип общеканальной сигнализации

Один общий канал сигнализации 64 кбит/с позволяет одновременно управлять соединениями около 4000 каналов информации (в ISDN это могут быть каналы передачи данных, разговорные каналы и др.). Так как каналы в ИКМ одинаковые, то легко выбрать в другом первичном тракте ИКМ резервный канал сигнализации.

17.2.2. Стек протоколов ОКС№7 в сети ТфОП/ISDN

На рис. 17.6 приведена схема стека протоколов ОКС№7 сети ТфОП/ ISDN в сопоставлении уровней модели OSI и уровней модели ОКС№7.

Подсистема передачи сообщений MTP (Message Transfer Part) включает три уровня ОКС№7- физический, канальный и сетевой. Два нижних уровня (физический MTP1 и канальный MTP2) так же как и в сети передачи данных X.25 полностью совпадает с моделью OSI. Уровень 1 в ОКС№7 называется звеном передачи данных, а уровень 2- звеном сигнализации (ЗС).

К подсистеме сетевого уровня ОКС№7 относится не только сетевой уровень MTP3, но SCCP (Подсистема управления соединениями сигнализации- Signaling Connection Control Part). Заметим, что функции 4-6 уровней модели OSI в модели ОКС№7 не требуют реализации. Подсистема пользователей ISDN, которая функционирует по протоколу ISUP, поддерживает сигнализацию телефонной сети и сети ISDN. Ранее для поддержания функций телефонного соединения использовался специальный протокол TUP (Telephone User Part), но в российской сети его функции выполняются с помощью ISUP.

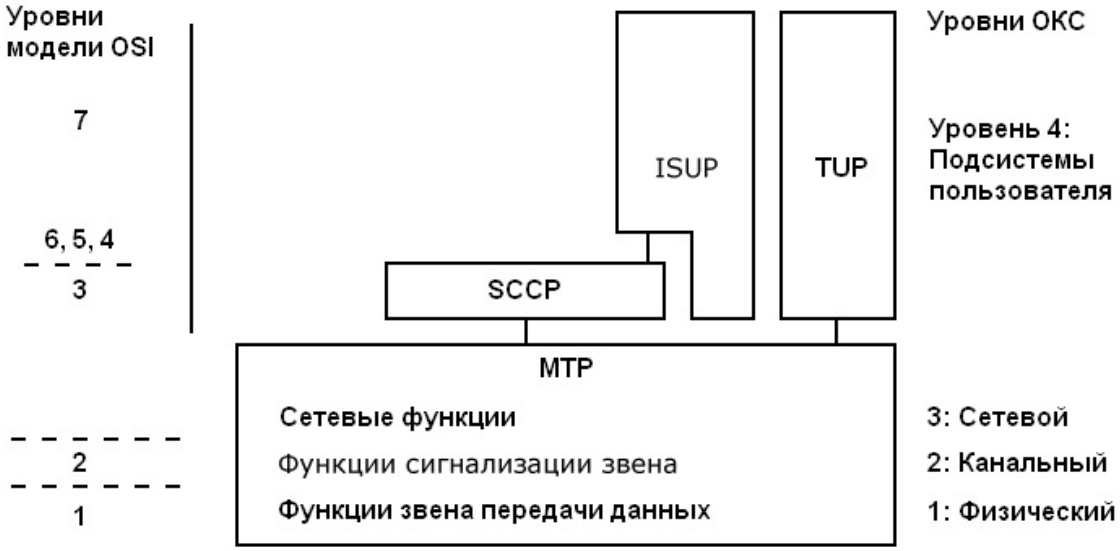


Рис. 17.6. Стек протоколов ОКС№7 в сети ТфОП/ISDN

17.2.3. Диаграмма установления соединения в системе ОКС№7 ISDN

На рис. 17.7 приведена диаграмма установления соединения в сети ISDN, включающая обмен сообщениями системы сигнализации ОКС№7. Процедура обмена сообщениями на абонентском доступе ISDN представлена в упрощенном виде по сравнению со схемой, приведенной ранее на рис. 17.3. Как видно из рис. 17.6 в подсистему пользователей модели ОКС№7 входят два протокола - протокол пользователя ISUP и протокол подсистемы управления соединениями сигнализации SCCP. Поэтому на диаграмме некоторые сообщения ОКС№7 относятся к ISUP, а некоторые к SCCP. Сигнализация в ОКС№7 показана на сети, состоящей из трех пунктов сигнализации, расположенных в двух оконечных узлах коммутации УК-А (АТС-А), УК-В (АТС-В) и одном промежуточном УК-П (АТС-П). Приведем краткое описание сообщений ISUP, участвующих в установлении соединения.

Начальное адресное сообщение IAM (Initial Address Message) - первое сообщение, передаваемое при установлении соединения, содержит адресную информацию. Эта информация записывается в IAM из поступившего сообщения абонентского доступа SETUP. В IAM записываются и другие информационные данные из SETUP. Узел коммутации УК-А определяет свободный информационный канал с промежуточным узлом коммутации (УК-П). Поле идентификации информационного канала в IAM занимает 2 байта. Если используется цифровой тракт 2,048 Мбит/с, то пять младших битов кодируют речевой временной интервал. Оставшиеся 7 битов используются для определения какому потоку ИКМ-30 принадлежит данный речевой интервал. Таким образом, один канал сигнализации 64 кбит/с позволяет одновременно устанавливать соединение максимум по 30*128, т.е. 3840 каналам.

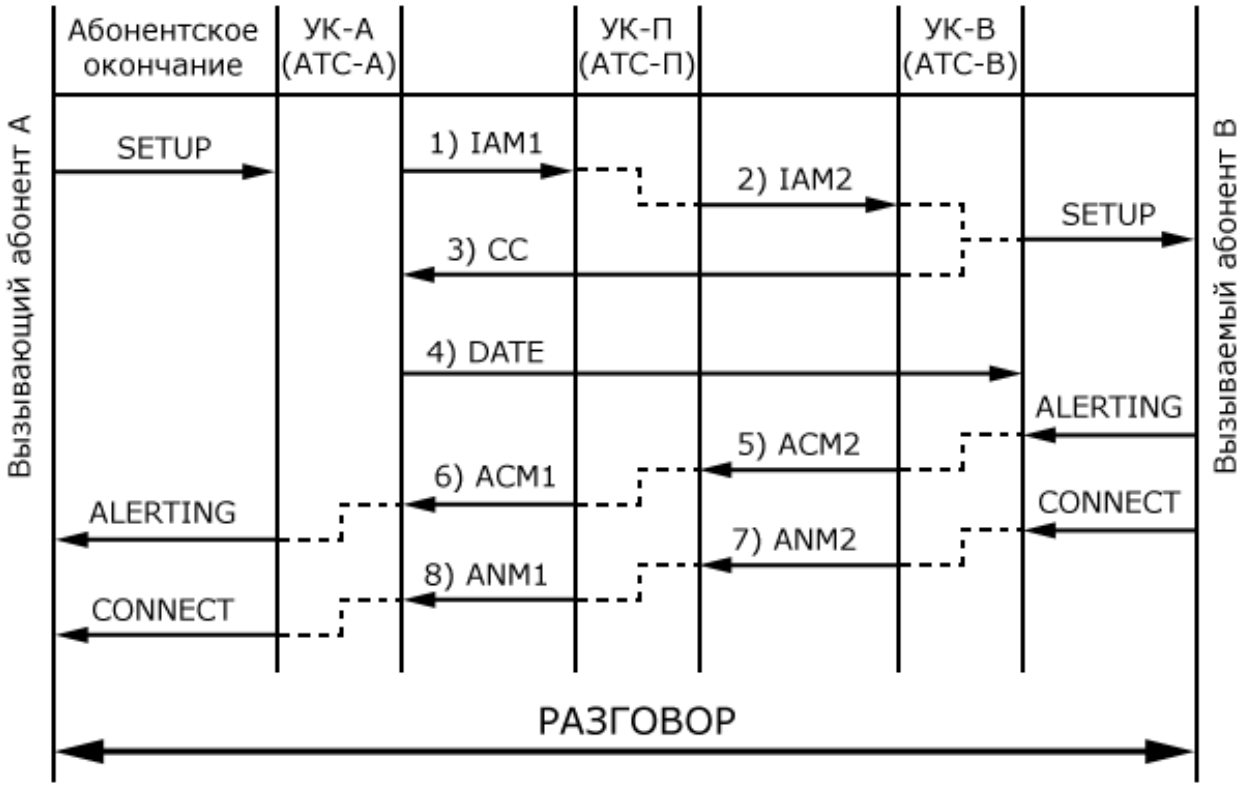


Рис. 17.7. Диаграмма установления соединения в системе ОКС№7 сети ТфОП/ISDN

Промежуточный узел коммутации УК-П принимает сообщение и в результате содержащейся в нем информации на основании таблицы маршрутизации определяет узел коммутации вызываемого абонента В, т.е. УК-В. Сообщение 1 (IAM), определяющее номер информационного канала между УК-А и УК-П на рис. 17.7 обозначено через IAM1. Узел коммутации УК-П определяет свободный информационный канал между УК-П и УК-В, заносит его в поле идентификации информационного канала. Полученное новое сообщение IAM2 направляется в УК-В. При поступлении IAM1 от УАК-А в УАК-П, и IAM2 в УК-В проключаются соответствующие разговорные тракты. Если требуется дополнительная информация, то на исходящую УК-А направляется сообщение 3 подтвердить соединение CC (Connection confirm) из конца в конец. Сообщение CC может включать, например, информацию для УК-А о дополнительных услугах, которые могут быть представлены с учетом возможностей абонента В. Промежуточный узел коммутации не анализирует эту информацию. Исходящий УК-А предоставляет соответствующую информацию в сообщении 4 также из конца в конец. Затем отправляются сообщения 5 и 6 о завершении приема адресной информации ACM (Address Complete Message), которое содержит информацию о статусе вызываемого абонента В (например, абонент свободен). Затем передаются сообщения 7 и 8 ответ абонента ANM (Answer Message). При этом входящий УК-В проключает разговорный тракт. При приеме сообщения ANM2 исходящий УК-А проключает разговорный

тракт. Таким образом, устанавливается соединение абонентов А и В, начинается тарификация и осуществляется разговор или передача данных. Сообщения ACM1 и ANM1 относятся к номеру информационного канала между УК-А и УК-П, а ACM2 и ANM2 – между УК-П и УК-В.

Отметим особенности сообщений 3 и 4 (из конца в конец на рис. 17.7). Функции этих сообщений обеспечиваются подсистемой управления соединением сигнализации SCCP, а не подсистемой ISUP (см. рис. 17.6). Подсистема SCCP была введена по многим причинам и в большей степени для обслуживания пользователей подвижной связи, интеллектуальной сети и др. Использование SCCP в сети ISDN не является ее основным назначением. Однако использование сообщений 3 и 4 в приведенной диаграмме (рис. 17.7) позволяет нам изложить некоторые из основных функций этой подсистемы SCCP. Необходимость внедрения SCCP была обусловлена тем, что в некоторых случаях желательно, чтобы сигнальные сообщения передавались от одного пункта к другому без проключения информационного канала. Одним из назначений подсистемы SCCP является обеспечение средств для возможности передачи блоков данных с использованием логических виртуальных соединений. Сообщения 3 и 4 иллюстрируют использование логических соединений. Установление логического соединения осуществляется с помощью двух сообщений:

- запрос соединения CR (Connection Request) от вызывающей стороны;
- подтверждение соединения CC (Connection Confirm) от вызываемой стороны.

В формате этих сообщений присутствует поле для условного номера. Эти условные номера также, как и номера логических каналов в сети X.25 служат для маршрутизации данных по установленному виртуальному каналу. В составе сообщений 1 и 2 (IAM1 и IAM2) содержится сообщение SCCP- запрос соединения CR с входящим в него исходящим условным номером LRNA. Сообщение 3 (CC) является сообщением SCCP (не входит ни в какое сообщение ISUP) и служит подтверждением соединения CC, в котором содержится исходящий условный номер LRNA и входящий условный номер LRNB. Теперь сообщения данных 4 и др. «из конца в конец» маршрутизируются по эти условным номерам. На рассмотренной диаграмме установление соединения приведено в упрощенном виде с использованием не всех типов сообщений ISUP и SCCP.

17.2.4. Протокол подсистемы передачи сообщений MTP

17.2.4.1. Уровни подсистемы передачи сообщений MTP

Рассмотрим процедуры, выполняемые каждым уровнем подсистемы передачи

(переноса) сообщений MTP. Поскольку система сигнализации ОКС№7 является сетью пакетной коммутации, приведем сравнение по функционированию с сетью передачи данных стандарта X.25. Стек уровней сети X.25 соответствует модели OSI. Поэтому такое сравнение преследует задачу упрощения описания функций ОКС№7. Подсистема MTP является общей для всех подсистем пользователя в одном пункте сигнализации. Функции MTP подразделяются на три уровня:

- функции звена данных сигнализации (уровень 1- физический);
- функции звена сигнализации (уровень 2- канальный);
- функции сети сигнализации (уровень 3- сетевой).

Как видно из рис. 17.6 сетевой уровень MTP не полностью соответствует сетевому уровню модели OSI.

17.2.4.2. Функции звена данных сигнализации (уровень 1, MTP1)

Звено данных сигнализации - это физическая среда для передачи битового потока между двумя пунктами в сети сигнализации. Протокол уровня 1 для звена данных сигнализации определен в рекомендации ITU-T Q.702 [39]. Цифровое звено данных сигнализации состоит из дуплексного канала передачи 64 Кбит/с, выделенного в цифровом тракте временного уплотнения 2,048 Мбит/с и оконечного оборудования, обеспечивающего интерфейс с сигнальным оборудованием. Стандартным канальным интервалом, используемым для звена данных сигнализации, является временной интервал 16. В отличие от X.25 аналоговые каналы в системе ОКС№7 не используются.

17.2.4.3. Функции звена сигнализации (уровень 2, MTP2)

Звено сигнализации (ЗС) ОКС№7 соответствует второму уровню модели OSI и обеспечивает безошибочную передачу сигнальных сообщений между двумя непосредственно соединенными пунктами сигнализации. Информация в ЗС передается в виде пакетов данных, называемых сигнальными единицами (SU-Signaling Unit). ОКС№7 является системой передачи данных с коммутацией пакетов.

Формат и функции MTP2 стандартизированы в документе ITU-T Q.703 [40].

Различают три типа СЕ:

- значащие сигнальные единицы ЗнСЕ или MSU (Message Signal Unit), которые используются для передачи информации подсистем ISUP и SCCP (смежных уровней с MTP), а также для передачи сообщений уровня MTP3 по выполнению

функций эксплуатационного управления сетью сигнализации;

- сигнальные единицы состояния ЗС LSSU (Link Status Signal Unit), которые используются для реализации функций второго уровня ОКС№7, т.е. MTP2.
- заполняющие сигнальные единицы FISU (Fill In Signal Unit), которые заполняют промежутки времени при отсутствии в ЗС сигнальных единиц MSU и LSSU. FISU выполняет функции повторной передачи MSU, которые не приняты противоположной стороной.

В форматы всех типов СЕ входят поля, выполняющие те же функции, что и на втором уровне X.25 (X.25/2):

- контрольно-проверочная комбинация циклического кода (с теми же полями, что и в X.25), по терминологии MTP это функция (и соответственно поле) обнаружения ошибок;
- параметры, обеспечивающие прием правильной последовательности сигнальных единиц. По терминологии MTP это функция (и соответственно поле) коррекции ошибок.

В отличие от X.25/2 в MTP2 предусмотрен контроль за качеством ЗС (т.е. канала передачи данных - в терминологии X.25/2). При обнаружении несоответствия определенным нормам ЗС выводится из обслуживания. Контроль качества ЗС производится непрерывно, т.е. при наличии информационных сообщений и при их отсутствии (в последнем случае за счет заполняющих СЕ, т.е. FISU). Контроль качества ЗС производится и при вхождении ЗС в связь (по терминологии ОКС№7 при фазировании).
Термин «сфазировано» применительно к звену сигнализации означает, что оно находится в таком состоянии, когда по нему можно производить обмен СЕ. Алгоритм процедуры начального фазирования предусматривает использование четырех типов СЕ состояния ЗС, т.е. LSSU с четырьмя видами индикации статуса фазирования SI (Service Indicator) для чего в формате LSSU по сравнению с FISU введено поле статуса 1-2 байта:

- SIO (Service Indicator “out of alignment”), не сфазировано;
- SIN (Service Indicator “normal”), нормальное фазирование;
- SIE (Service Indicator “emergency”), аварийное фазирование;
- SIOS (Service Indicator “out of service”), вне обслуживания.

Фазирование применяется при первоначальном включении ЗС или после восстановления из-

за сбоя. Процедурой фазирования предусмотрено два вида проверок качества передачи по ЗС: для нормального и для аварийного режима. Нормальный режим применяется, когда кроме проверяемого ЗС в пучке ЗС есть и другие доступные. При аварийном периоде таких ЗС нет. Под пучком звеньев сигнализации SLS (Signaling Link Set) понимается одно или несколько ЗС между двумя соединенными напрямую пунктами сигнализации.

1. Подсчет коэффициента ошибок сигнального звена

Рассмотрим процедуру подсчета коэффициента ошибок сигнального звена. При обнаружении случаев нарушения фазирования или ошибочной передачи сигнальных единиц звено не выводится из работы до тех пор, пока специальной процедурой подсчета не будет установлено, что коэффициент ошибок достиг порогового значения. На основании данных о превышении порога интенсивности ошибок передачи, полученных с уровня MTP2, на уровне MTP3 принимается решение о выведении звена из обслуживания для проведения повторного начального фазирования и проверки. Процедура подсчета ошибок реализует две функции: подсчет коэффициента ошибок при передаче сигнальных единиц и подсчет коэффициента ошибок при фазировании звена. Приведем процедуру подсчета коэффициента ошибок при передаче сигнальных единиц (SUERM, Signal Unit Error Rate Monitor) для оценки интенсивности ошибочной передачи сигнальных единиц, когда сигнальное звено находится в работе.

Процедура SUERM отслеживает количество случаев нарушения фазирования, оперируя тремя следующими параметрами:

- количество T сигнальных единиц, последовательно принятых с ошибкой и вызывающих индикацию высокой интенсивности ошибок уровню MTP3;
- наименьшей интенсивностью ошибок 1/D (отношение количества ошибочных сигнальных единиц к общему количеству сигнальных единиц), при которой уровень MTP3 извещается о высокой интенсивности ошибок;
- количеством N байт, когда счетчик увеличивает свое значение на единицу через каждые N байт, принятых до получения правильной сигнальной единицы.

  При включении звена значение счетчика равно нулю. Для звеньев со скоростью 64 Кбит/с установлены следующие значения параметров процедуры SUERM:

  T=64 сигнальных единиц;

  D=256;

  N=16 октетов.

  Для этих величин время перехода на резервное звено в случае потери

фазирования составит примерно 128 мс при скорости 64 Кбит/с.

2. Управление режимами “отказ процессора” и “ перегрузка в канале”

Отметим еще одну особенность MTP2 по сравнению с X.25/2. В отличии от X.25/2 используется процедура для обработки ситуации отказа процессора на сетевом уровне MTP3. В случае отказа MTP3 или подсистемы пользователя индикация этого события направляется смежному пункту сигнализации посредством LSSU с индикатором статуса «отказ процессора» SIPO (Service Indicator «processor outage”). Приняв SIPO, пункт сигнализации прекращает передачу MSU и начинает передавать FISU. Посредством специальной выдержки времени (40-50 сек) уровень MTP3 смежного пункта сигнализации контролирует длительность пребывания ЗС в состоянии отказа и, в случае превышения порога, выводит ЗС из обслуживания и подвергает его процедуре начального фазирования.

В стандарте X.25/2 рассматривается необходимость обработки ситуации возникновения перегрузки на втором уровне. Поскольку в MTP2 рассматриваются обе ситуации (и возникновение перегрузки и отказ процессора MTP3), то в этом случае предусмотрен алгоритм их различия передающей стороной. Не следует смешивать данную процедуру, применимую только для управления потоком по одному звену, с процедурами управления потоком сигнального трафика в случае перегрузки одной из подсистем пользователей или всего пункта сигнализации, которые относятся к функциям MTP3.

3. Коррекция ошибок.

Функция обеспечения в сети X.25 правильной последовательности сообщений в ОКС№7 называется другим термином - коррекция ошибок.

В ОКС№7 на втором уровне предусмотрено два метода коррекции ошибок - базовый метод (BEC-Basic Error Correction) и метод превентивного циклического повторения (PCR-Preventive Cyclic Rertransmission). Базовый метод применяется для ЗС, в которых время распространения менее 15 мсек. Алгоритм базового метода мало отличается от алгоритма на канальном уровне X.25. Вместо супервизорных кадров положительной или отрицательной квитанции в ОКС№7 в составе всех типов СЕ используются прямой и обратный бит-индикаторы. Алгоритм несложный и описан в рекомендации ITU-T Q.702 [36].

Метод превентивного циклического повторения предусматривает повторную передачу неподтвержденных СЕ циклически в течение времени, когда нет новых значащих

сигнальных единиц ЗнСЕ (MSU), сигнальных единиц состояния звена LSSU. Под нумерацию ЗнСЕ выделено 7 бит, т.е. порядковые номера от 0 до 127. Если достигнут предел количества ЗнСЕ, то используется процедура превентивного (вынужденного) повторения. Передача новых СЕ прекращается, а все ЗнСЕ, хранящиеся в буфере повторной передачи, передаются до тех пор, пока не уменьшится число неподтвержденных СЕ.

Метод превентивного циклического повторения применяется на межконтинентальных сигнальных звеньях, в которых задержка распространения в одном направлении больше или равна 15 мс, а также на звеньях, организованных в спутниковых системах передачи.

Функции MTP2 реализуются на сигнальном терминале (канальном процессоре в терминологии X.25/2), подключенном так же, как и в сети X.25 к центральному процессору, выполняющему функцию сетевого уровня (MTP3).

17.2.4.4. Функции сети сигнализации (уровень 3, MTP3)

Функции сети сигнализации относятся к обмену сообщениями между пунктами сигнализации, являющимися узлами сети сигнализации. Эти функции и процедуры осуществляются подсистемой передачи (переноса) сообщений на уровне MTP3. Функции сигнализации подразделяются на две основные категории:

- обработка сигнальных сообщений;
- управление сетью сигнализации.

Эти функции узла сети сигнализации выполняются центральным процессором, как и функция коммутации в центре коммутации пакетов сети X.25. Обработка сигнальных сообщений выполняет следующие функции:

- маршрутизация сообщений;
- распознавание сообщений;
- распределение сообщений.

Формат и функции сообщений MTP3 стандартизированы в документе ITU-T Q.704 [41]. Уровень X.25/3 так же, как и MTP3 выполняет маршрутизацию сообщений. Однако в протоколе сети X.25 эта функция не стандартизирована. Функция распознавания сообщений используется для определения предназначено ли оно для обработки на данном пункте или должно быть направлено на процедуру маршрутизации. В стандарте MTP3 выполняются следующие функции распределения сообщений. Сообщения MTP3 либо подлежат обработке

этим уровнем, либо передаются для обработки одной из подсистем (ISUP, SCCP, TUP). MTP3, кроме маршрутизации поступивших сообщений может выполнять функции управления сетью или тестирования звена сигнализации. Функции управления сетью сигнализации - это обеспечение реконфигурации сети в случае отказа и управление трафиком при перегрузке. Для этого используются процедуры изменения маршрута сигнального трафика. При этом между пунктами сигнализации происходит обмен определенными сообщениями. Функции управления сетью передачи данных отсутствуют в стандарте X.25/3.

Рассмотрим отдельно функции сигнализации по обработке сигнальных сообщений и по управлению сетью сигнализации. В формат сообщений MSU, выполняющих эти функции входят следующие поля (рис. 17.8):

- поле обнаружения ошибок и поле коррекции ошибок (также как и в сообщениях LSSU и FISU);
- поле байта служебной информации SIO;
- поле сигнальной информации SIF;
- флаг (Flag), отмечающий начало или конец каждой сигнальной единицы. В качестве флага используется байт 01111110.

Рис. 17.8. Формат сообщения MSU

17.2.4.5. Функции обработки сигнальных сообщений

Рассмотрим функции маршрутизации, распознавания и распределения сообщений MTP3. Для этого раскроем содержимое полей SIO и SIF сообщения MSU. Поле SIO (Service Information Octet) – байт, указывающий на принадлежность информации сообщения конкретной подсистеме. SIO состоит из индикатора вида службы SI (Service

Indication) и из четырех бит индикатора сети NI (Network Indication). SI указывает (распределяет) к какой из следующих подсистем относится сообщение MSU:

- ISUP;
- SCCP;
- управление сетью сигнализации;
- тестирование звена сигнализации (3С);
- TUP.

Индикатор сети NI из двух бит в поле SIO позволяет определить какой сети принадлежит сообщение. В ТфОП/ISDN РФ приняты следующие индикаторы:

- NI=11 для местной сети;
- NI=10 для междугородной сети;
- NI=00 для международной сети.

Поле сигнальной информации SIF (Signaling Information Field) при выполнении функции обработки сигнальных сообщений включает инкапсулированное сообщение подсистемы пользователя (ISUP, SCCP или TUP). Поле SIF переменной длины и состоит из переменного числа байт (не менее 2 и не более 272). В старшие биты этого поля входит этикетка маршрутизации, которая служит для маршрутизации сообщения или распознавания принятого сообщения в пункте назначения с целью передачи его в подсистему пользователя, к другому пункту сигнализации.

Этикетка маршрутизации состоит из трех полей:

- код пункта назначения DPC (Destination Point Code);
- код исходящего пункта OPC (Originating Point Code);
- поле выбора (селекции) звена сигнализации SLS (Signaling Link Selection). SLS принадлежит сообщениям ISUP, TUP, SCCP. В сообщениях управления сетью это поле выполняет другие функции и называется SLC.

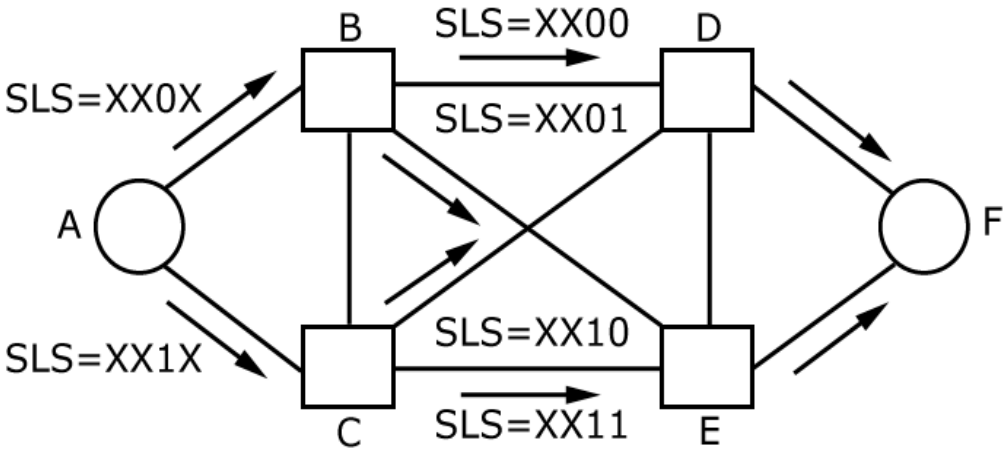
Как правило, пункт сигнализации назначения может быть доступен исходящему пункту сигнализации по нескольким возможным путям. Поэтому при маршрутизации в ОКС№7 на уровне MTP3 применяют методы разделения сигнальной нагрузки. Разделение нагрузки по различным соединительным путям осуществляется с помощью поля SLS , которое имеет различные коды для различных путей передачи сигнальных сообщений. SLS используется также для разделения нагрузки между звеньями сигнализации одного пучка. На

рис. 17.8. приведен формат значащей сигнальной единицы MSU, выполняющей функцию MTP3 по обработке сигнальных сообщений: а) сообщений пользователя, б) сообщений управления сетью сигнализации.

17.2.4.5.1. Маршрутизация сигнальных сообщений

Сигнальный маршрут (SR- Signaling Routing)- это заранее установленный путь от исходящего пункта к пункту назначения, состоящий из транзитных пунктов сигнализации, последовательно соединенными пучками ЗС. Под пучком ЗС понимается использование нескольких ЗС между смежными пунктами сигнализации. Совокупность всех маршрутов между исходящим пунктом и пунктом назначения называется пучком сигнальных маршрутов (SRS- Signaling Route Set).

На рис. 17.9 приведен пример маршрутизации при отсутствии отказов для сообщений поступающих из пункта сигнализации A в пункт сигнализации F. При распределении трафика для разделения нагрузки в исходящем пункте сигнализации и промежуточных транзитных пунктах сигнализации используют поле селекции звена сигнализации SLS. Эту селекцию необходимо выполнять так, чтобы трафик между всеми доступными маршрутами



был распределен равномерно.

Рис. 17.9. Пример идентификации с помощью SLS маршрута в пучке сигнальных маршрутов

Распределение нагрузки в исходящем пункте (A) и транзитных пунктах (B,C,D,E) производится на основании поля SLS по четырем маршрутам. Исходящий пункт A использует второй значащий бит поля SLS, а транзитные пункты B и C – первый. Выбор звена для маршрутизации в обратном направлении от F к A делается в каждом пункте

независимо от маршрутизации в прямом направлении. Например, в прямом направлении сигнальные сообщения, относящиеся к одной и той же сигнальной процедуре, в одном направлении проходят по маршруту A-C-D-F, а в обратном - по маршруту F-E-B-A. Звенья BC и DE используются только в случае отказа других звеньев и пунктов.

Приведем все четыре маршрута от A к F при нормальной маршрутизации, т.е. в отсутствии отказов ЗС или пунктов сигнализации. В скобках указаны состояния поля SLS транзитных пунктов сигнализации (B или C) по каждому маршруту от A в F в сообщениях, поступающих в пункт назначения.

A-B-D-F (SLS=xx00)

A-C-D-F (SLS=xx10)

A-B-E-F (SLS=xx01)

A-C-E-F (SLS=xx11)

При отсутствии отказов звеньев сигнализации BC и DE не используются.

Приведенная структура на рис. 17.9 рекомендована в качестве базовой при построении международной сети ОКС№7.

Приняты следующие допущения относительно схемы маршрутизации для базовой структуры:

- основной маршрут должен содержать минимальное число транзитных пунктов;
- если имеется несколько маршрутов, доступных для переноса сообщения, то используется разделение нагрузки между ними.

Для предотвращения возможных аварийных ситуаций в каждом пункте сигнализации имеется информация о резервном маршрутировании, которая определяет для каждого из нормальных ЗС один или несколько резервных пучков ЗС, когда нормальные ЗС больше не являются доступными. В таблице 17.1 приведен перечень резервных пучков ЗС для схемы маршрутизации рис. 17.9 в условиях отказов. Таблица составлена только для двух пунктов сигнализации (A и B) этой схемы. При отсутствии отказов применяется разделение нагрузки между основным и резервным пучком (альернативным) ЗС. Резервные пучки приоритета 2 используются только тогда, когда все основные и резервные пучки ЗС первого приоритета недоступны.

Приоритет 1 - используется, когда основной набор звеньев работает в режиме с разделённой нагрузкой и в отсутствии неисправностей

Приоритет 2 - используется, когда все наборы звеньев с приоритетом 1 становятся недоступными

Таблица 17.1. Резервные пучки сигнальных звеньев в пунктах сигнализации A и B с учетом приоритета

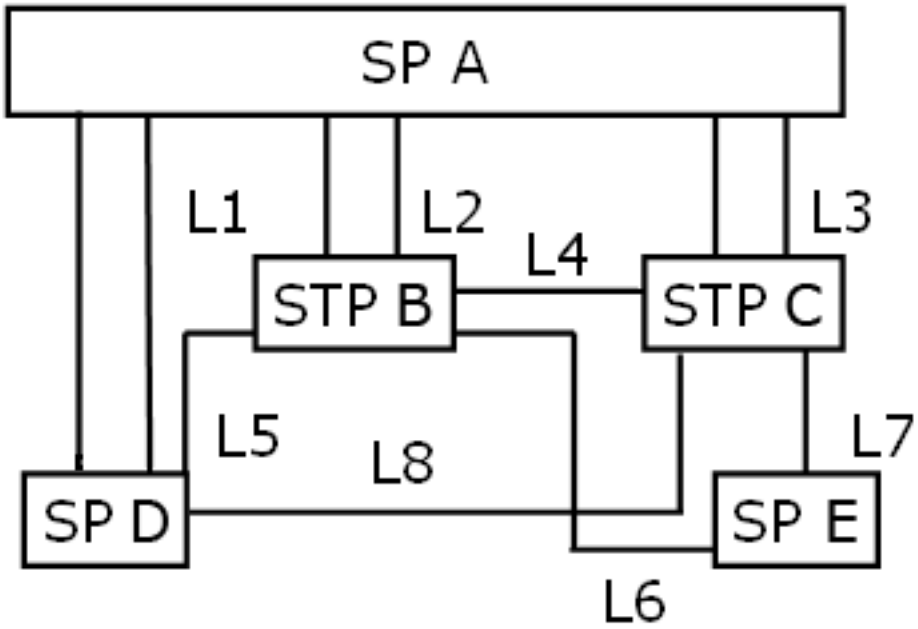


Рис. 17.10. Пример структуры сети ОКС№7

Как видно из рис. 17.10 пример структуры сети ОКС№7 включает три SP (SP A, SP E, SP D), два STP (STP B, STP C) и пучки звеньев сигнализации (L1-L8). Некоторые из пучков ЗС (L4-L8) состоят из одного звена, а остальные (L1-L3) из двух ЗС. В таблице маршрутизации введены следующие обозначения:

Li, Lj: Li- нормальный пучок ЗС, Lj- резервный пучок ЗС;

Li-Lj: разделение нагрузки между пучками ЗС Li и Lj.

Каждая строка является таблицей маршрутизации для соответствующего пункта сигнализации (исходящего или транзитного).

Для примера приведем на основании таблицы маршрут сообщений подсистемы пользователя от SP A в SP E в случае отсутствия отказов пучков ЗС.

1. Сообщения направляются с разделением нагрузки по пучкам ЗС L2 и L3 (см. строку таблицы маршрутизации для SP A).
2. Сообщения из STP B поступают на ЗС L6 и далее в SP E.
3. Сообщения из STP C поступают на ЗС L7 и далее в SP E.

Таким образом, пучок маршрутов состоит из двух маршрутов, каждый из которых включает один транзитный пункт сигнализации:

1. SP A-STP B-SP E;
2. SP A-STP C-SP E.

В обратном направлении сигнальные сообщения поступают по маршруту SP E-STP C-SP A. При отказе ЗС L3 и L6 пучок маршрутов состоит из одного резервного маршрута SP A-ST B-STP C-SP E, который включает два транзитных пункта сигнализации через альтернативные звенья сигнализации второго приоритета. Обратный маршрут совпадает с прямым. В некоторых случаях отказов ЗС для маршрутизации недостаточно только данных таблицы маршрутизации. В случае отказа L6, L7, L4 нет ни одного доступного маршрута сообщениям из SP A в SP E. О недоступности SP E, STP C и STP B сообщают SP A специальными сообщениями управления сетью сигнализации. В таблице маршрутизации SP A отмечается недоступность ЗС L2 и L3 по причине недоступности SP E.

17.2.4.6. Требования к показателям качества обслуживания MTP

В Рекомендациях ITU-T Q.706 [43] приведены следующие показатели QoS подсистемы MTP. Высокая степень централизации функций сигнализации является причиной высоких требований к количественным значениям этих показателей:

1. время неготовности пучка маршрутов сигнализации не должно превышать в сумме 10 минут в год, т.е. $\geq 0{,}99998$. Под пучком сигнальных маршрутов понимается совокупность всех маршрутов между исходящим пунктом и пунктом назначения;
2. коэффициент потери сигнальных сообщений из-за отказа подсистемы MTP должна быть ниже 10^{-7};
3. вероятность передачи сигнального сообщения в неправильной последовательности должна быть ниже 10^{-10};
4. вероятность приема сигнальной единицы с необнаруженной ошибкой должна быть ниже 10^{-10}, т.е. не более одной ошибки на 10^{10} всех ошибок в сигнальных единицах, не обнаруженной MTP.
5. среднее значение нагрузки на одно звено сигнализации не должно превышать 0,2 Эрланга. Эрланг- это безразмерная единица измерения интенсивности трафика. В общем случае средняя интенсивность трафика вычисляется по формуле $A = \lambda * T$, где λ- среднее число вызовов в час,T- продолжительность одного соединения. Например,

при числе вызовов в ча=3 и продолжительности разговора Т= 4 мин, средняя нагрузка на линии равна 0,2 Эрл. Допускается увеличение нагрузки до 0,4 Эрл в ситуациях сбоев или перегрузок при переходе на резервные звенья сигнализации и альтернативные маршруты;

6. интенсивность ошибок на один бит в ЗС должен быть ниже 10^{-6} для длительных интервалов и ниже 10^{-4} для коротких интервалов.

17.3. Подсистема пользователя ISUP

Прикладная подсистема пользователя ISUP (Integrated Service User Part) сети ISDN обеспечивает запросы пользователей ТфОП и ISDN на установление коммутируемых соединений. Подсистема ISUP специфицирована в рекомендации Q.767 [44,45]. Вариант протокола ISUP, учитывающий специфику сети ТфОП России называется ISUP-R. Протокол ISUP-R включает в себя 22 услуги:

- конференцсвязь;
- удержание соединения (возможность прервать разговорную фазу с последующим восстановлением);
- переадресация вызова;
- определение номера вызывающего абонента;
- запрещение идентификации номера вызывающего абонента;
- извещение о стоимости вызова по его завершении и др.

Сигнальная информация (т.е. сообщения по установлению или разъединению соединения) передается в поле SIF (рис.17.8) значащей сигнальной единицы и включает:

- тип сообщения ISUP, осуществляющего управление вызовом, между абонентами сети ISDN. Общее число типов сообщений ISUP двадцать девять. Некоторые из этих сообщений были приведены выше на диаграмме рис. 17.7. Каждое сообщение ISUP имеет обязательные и необязательные параметры (номер вызываемого абонента, номер вызывающего абонента и др.);
- код идентификатора канала CIC (Circuit Identification Code), указывающий номер разговорного канала между двумя станциями. Пять младших бит CIC кодируют речевой временной интервал цифрового тракта 2,048 Мбит/с, а 7 бит используются для определения какому ИКМ - потоку принадлежит данный речевой интервал.

На рис. 17.11 приведен пример установления и разъединения соединения подсистемой ISUP.

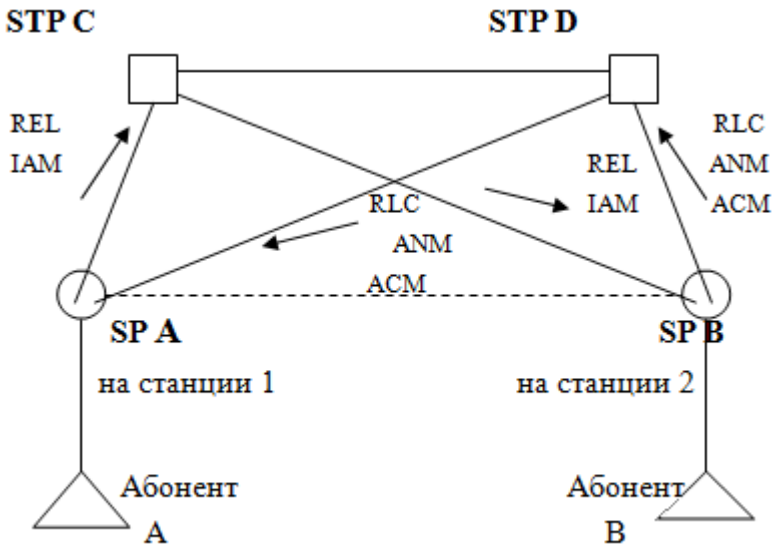


Рис. 17.11. Пример установления и разъединения соединения подсистемой ISUP

В рассматриваемом примере вызывающий абонент А набирает номер и направляет вызов к вызываемому абоненту В. При этом в базовой сети связи и в сети сигнализации осуществляются перечисленные ниже действия.

1. Станция 1 анализирует набранный номер и определяет, что вызов должен быть маршрутизирован станции 2.
2. Станция 1 выбирает свободный разговорный тракт к станции 2 и формирует начальное адресное сообщение IAM. В сообщении определены код исходящего пункта сигнализации на станции 1, код пункта назначения на станции 2, выбранный разговорный тракт, номера вызывающего и вызываемого абонентов, а также другая информация, не рассматриваемая в данном примере.
3. SP A на станции 1 выбирает одно из звеньев сигнализации (например, звено АС) и передает по нему сообщение IAM для маршрутизации в SP B на станции 2.
4. STP C принимает сообщение, анализирует его этикетку маршрутизации и определяет, что сообщение должно быть маршрутизировано к SP B на станции 2. Сообщение передается по звену сигнализации СВ.
5. SP B принимает сообщение, анализирует его и определяет, что данное сообщение

относится к вызываемому абоненту B и данный номер находится в состоянии «свободен».

6. SP B формирует сообщение ACM о принятии полного адреса, которое означает, что сообщение IAM корректно достигло пункта назначения. В сообщении определены код пункта назначения SP B, код исходящего пункта SP A и выбранный разговорный тракт.
7. SP B выбирает одно из 3C (например, звено BD) и передает по нему сообщение ACM для маршрутизации к SP A. Одновременно станция 2 проключает разговорный тракт в обратном направлении к станции 1, посылает тональный сигнал по этому тракту и посылает звонок по линии к вызываемому абоненту B. На рисунке разговорный тракт показан пунктирной линией.
8. STP D принимает сообщение, анализирует его этикетку маршрутизации и определяет, что сообщение должно быть маршрутизировано к SP A на станции 1. Сообщение передается по звену сигнализации DA.
9. После получения сообщения ACM станция 1 подсоединяет линию абонента A к выбранному разговорному тракту. Вызывающий абонент A слышит сигнал звонка, посланного станцией 2 вызываемому абоненту B.
10. В момент снятия трубки вызываемым абонентом B пункт сигнализации SP B на станции 2 формирует сообщение «ответ абонента» ANM. В сообщении определены код пункта назначения SP A, код исходящего пункта SP B и выбранный разговорный тракт.
11. SP B выбирает для передачи сообщения ANM то же звено сигнализации BD, что и для передачи сообщения ACM. К этому моменту разговорный тракт подключен к абонентским линиям.
12. STP D принимает сообщение, анализирует его этикетку маршрутизации и определяет, что сообщение должно быть маршрутизировано к SP A на станции 1. Сообщение передается по звену DA.
13. Станция 1 проверяет, что вызывающий абонент A подсоединен к исходящему разговорному тракту и что разговор абонентов может осуществляться.
14. Если вызывающий абонент A кладет трубку первым, то SP A на станции 1 генерирует сообщение REL, адресованное SP B на станции 2, об освобождении разговорного тракта, ассоциированного с данным вызовом. SP A посылает данное сообщение по звену сигнализации AC.
15. STP C принимает сообщение, анализирует его этикетку маршрутизации и определяет, что сообщение должно быть маршрутизировано к SP B. Сообщение передается по звену CB.

16. SP B принимает сообщение REL, станция 2 отсоединяет разговорный тракт от линии вызываемого абонента B, возвращает разговорный тракт в состояние «свободен», SP B генерирует сообщение RLC об окончании освобождения тракта и посылает его по звену сигнализации BD.
17. STP D принимает сообщение, анализирует его этикетку маршрутизации и определяет, что сообщение должно быть маршрутизировано к SP A. Сообщение передается по звену DA.
18. Получив сообщение RLC, станция 1 возвращает разговорный тракт в состояние «свободен».

17.4. Аутентификация пользователя в сети ISDN

В сети ISDN используется один из наиболее простых методов однопроходной аутентификации с помощью пароля, обычно называемого *PIN-кодом (Personal Identification Number)* многоразового использования или пароля одноразового использования *TAN (Transaction Number)*. Под однопроходным методом аутентификации пользователя понимается проверка подлинности желающего подключиться к сети пользователя по результатам анализа принятого от него одного сообщения аутентификации. В настоящем разделе рассмотрены процедуры такой аутентификации в сетях связи ISDN. Пароль, поступающий от пользователя, сравнивается с паролем, хранящимся в сети. Аутентификация считается успешной, если оба значения совпадают.

17.4.1. Аутентификация пользователя с помощью PIN-кода

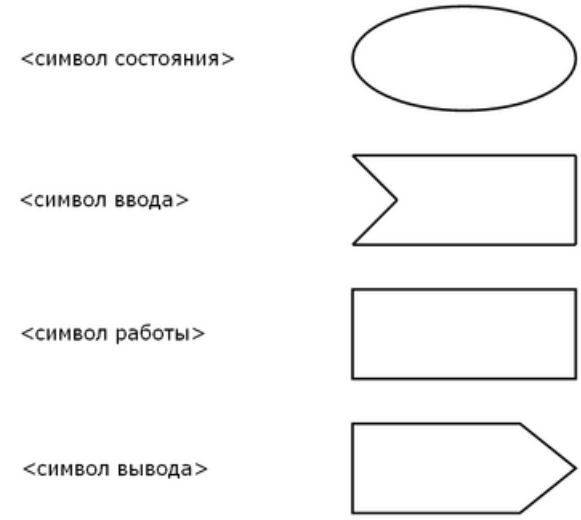
Для сети ISDN в соответствии с документом ETSI [46] PIN-код состоит минимум из четырех и максимум из 12 символов. Защита от несанкционированного доступа пользователя к сети абонентского доступа DSS1 ISDN обеспечивается:

- секретностью PIN-кода;
- процедурой предоставления пользователю возможности сменить значение PIN-кода.

Приведем описание процедур смены значения PIN-кода по запросу пользователя.

На рис. 17.12 на двух листах приведены процедуры управления со стороны пользователя механизмов аутентификации PIN в сети абонентского доступа DSS1 ISDN. На рис. 17.13 на двух листах приведены процедуры управления со стороны сети механизмов аутентификации PIN в сети абонентского доступа DSS1 ISDN. Указанное описание приведено с помощью диаграмм языка спецификации и описания SDL (Specification and Description Language) в

соответствии с рекомендацией ITU-T Z.100 [47]. В соответствии с указанной рекомендацией принята следующая графическая грамматика.



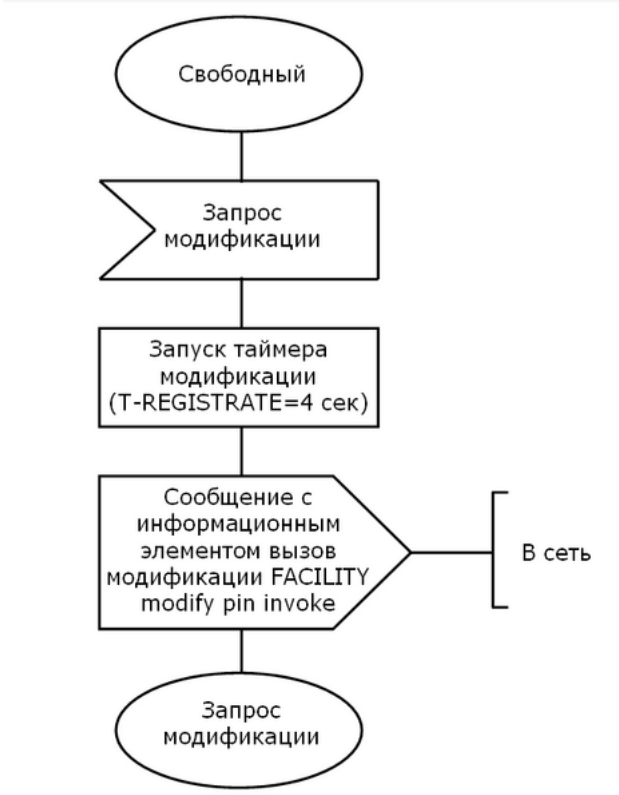


Рис. 17.12. (лист 1). Процедуры управления механизмом безопасности PIN со стороны пользователя

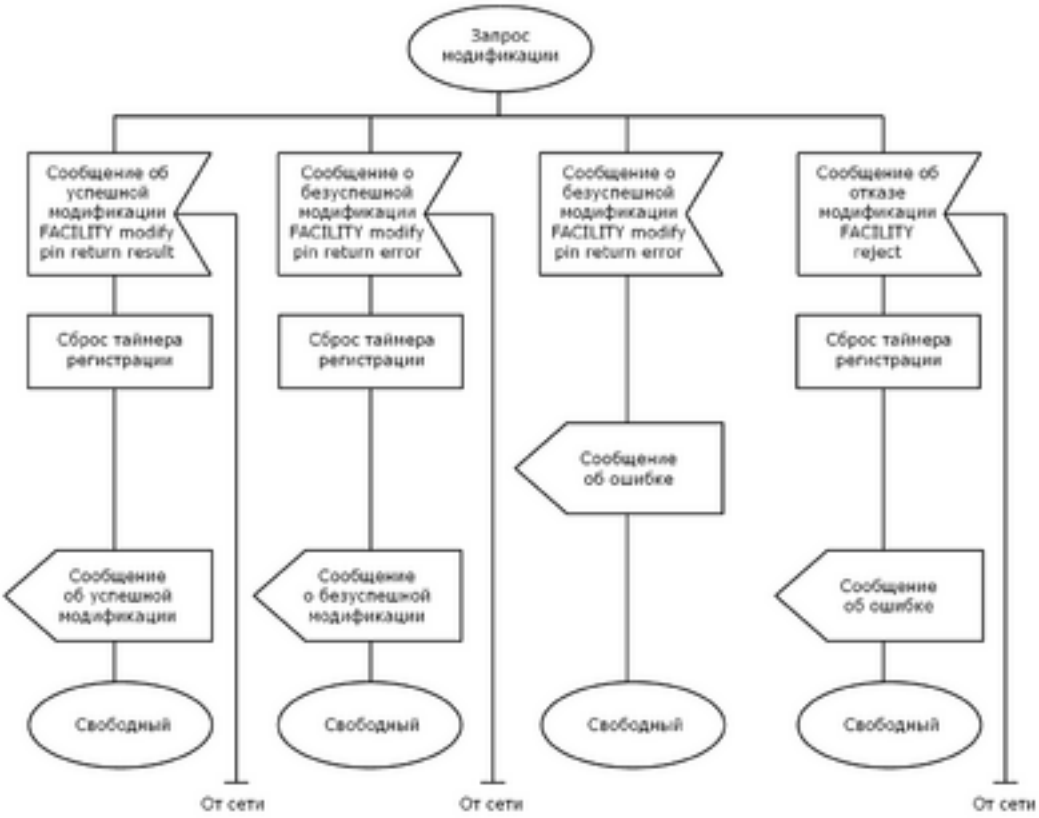


Рис. 17.12. (лист 2). Процедуры управления механизмов безопасности PIN со стороны пользователя

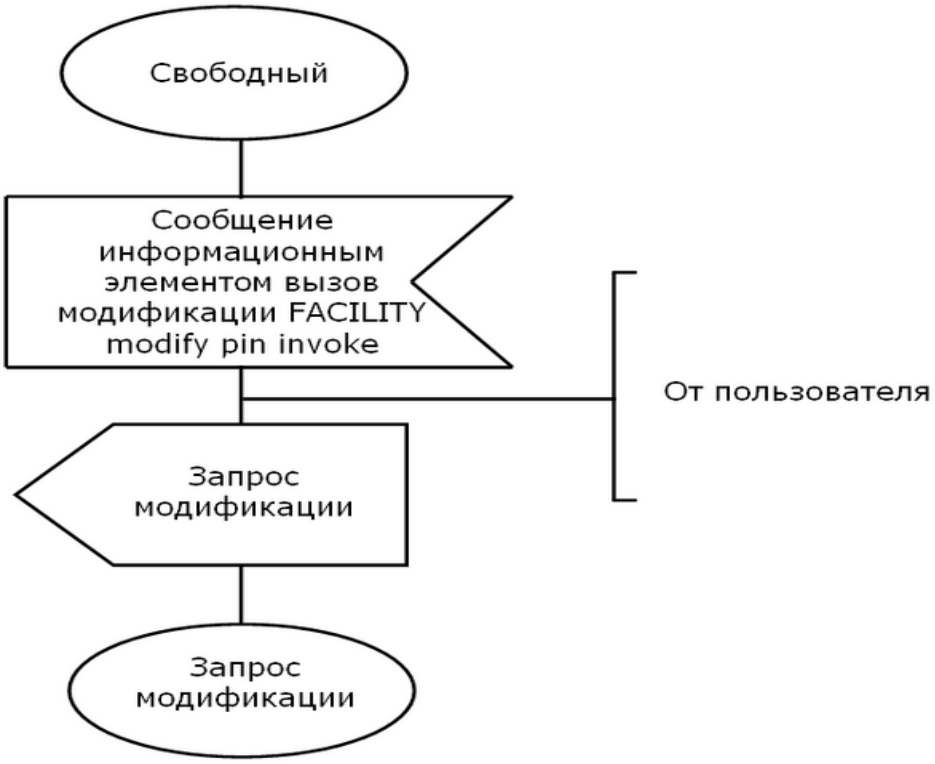


Рис. 17.13. (лист 1). Процедуры управления механизмом безопасности PIN со стороны сети

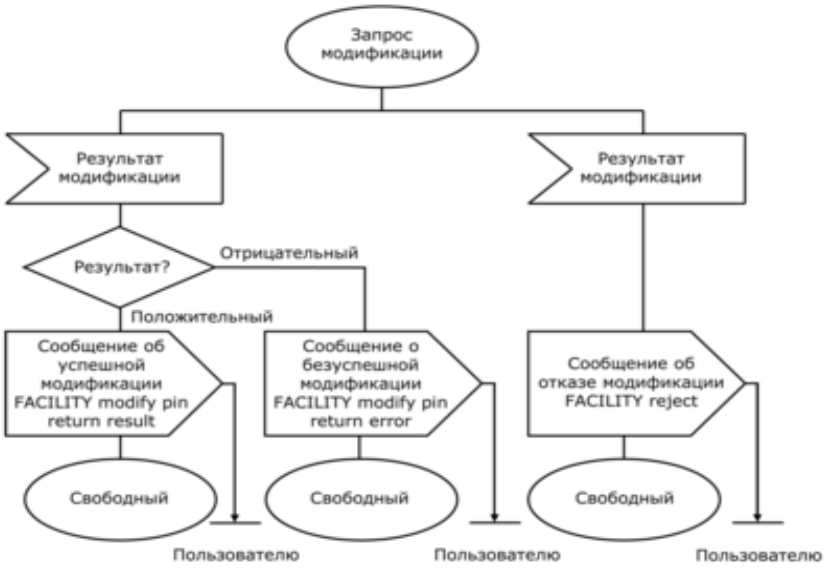


Рис. 17.13. (лист 2). Процедуры управления механизмом безопасности PIN со стороны сети

Как видно из диаграммы рис. 17.12. (лист 1), на стороне пользователя, находящегося в состоянии «свободный», выполняется следующая последовательность операций:

- ввод команды «Запрос модификации» PIN-кода;

- запуск таймера регистрации на время 4 сек. (T-REGISTRATE = 4 сек.);
- передача в сеть сообщения с информацией о запросе на регистрацию PIN-кода (FACILITY modify pin invoke);
- переход в состояние «Запрос модификации».

Сетевое окончание абонентского доступа DSS1 сети ISDN, находящееся в состоянии «Свободный», как видно из диаграммы рис. 13 (лист 1) выполняет следующую последовательность операций:

1. прием от пользователя сообщения с информацией о запросе на регистрацию PIN-кода;
2. передача этого сообщения на обработку;
3. переход в состояние «Запрос модификации».

Пользователь выполняет (рис. 17.12 (лист 2)) следующие операции после получения приведенных выше сообщений от сетевого окончания:

1. при приеме сообщения об успешной модификации производится сброс таймера регистрации и пользователь оповещается о результате модификации;
2. при приеме сообщения о безуспешной модификации производится сброс таймера модификации и пользователю сообщается причина;
3. при срабатывании таймера модификации пользователю передается сообщение об этом;
4. при приеме сообщения об отказе модификации производится сброс таймера модификации и пользователю в этом сообщении указывается причина.

Сетевое окончание выполняет следующие операции (рис. 17.13 (лист 2)) после обработки результата принятого сообщения:

1. при положительном результате пользователю передается сообщение об успешном завершении модификации PIN-кода (FACILITY modify pin return result) и новый PIN-код с одновременным переходом в состояние «Свободный»;
2. при отрицательном результате пользователю передается сообщение о безуспешной модификации (FACILITY modify pin return error) с одновременным переходом в состояние «Свободный».

Приведем некоторые из возможных причин безуспешной модификации PIN-кода:

– ошибочные данные в сообщении пользователя «Запрос модификации»;
– недействительный адрес пользователя;

- PIN-код не соответствует текущему (подлежащему замене) PIN- коду;
- новый PIN-код равен текущему PIN-коду.

Как показано на диаграмме, возможен отказ в модификации PIN-кода с последующей передачей соответствующего сообщения (FACILITY reject) пользователю. Приведем некоторые из возможных причин передачи такого сообщения:

1. пользователь превысил допустимое число M подряд безуспешных запросов на модификацию PIN-кода;
2. пользователь не подписан на предоставление аутентификации для конкретной услуги сети.

17.4.2. Аутентификация пользователя с помощью TAN

При использовании процедуры аутентификации с помощью PIN-кода возможна незаконная аутентификация злоумышленника в результате повтора им «сообщения аутентификации». Шифрование этого сообщения вместе с входящим в него PIN-кодом не защищает от этой угрозы повтора. Использование в ISDN одноразового пароля TAN (Transaction Number) обеспечивает защиту от этой угрозы. Каждый пользователь и сеть для определенной услуги (или нескольких услуг) ISDN содержат списки одноразовых паролей TAN под номерами. Например, под номером 100 значится сгенерированное случайное число от 6 до 12 знаков. Алгоритм формирования каждого TAN на сетевом окончании абонентского доступа DSS1 должен быть одним и тем же, что и пользователя. Во время процедуры аутентификации пользователя пароль TAN используется один раз из этого списка. Когда использование паролей списка завершается, пользователь и сеть формирует новый список TAN.

17.5. Аутентификация объектов аудиовизуальной службы сети ISDN и создание общих секретных ключей взаимодействующих объектов

Согласно докладу на второй международной конференции по безопасности сетей связи [48] еще в прошлом веке в сети связи общего пользования ISDN Англии обеспечивалось шифрование речи и данных. Такая же услуга была создана и на сети ССОП ISDN немецкого оператора Deutschen Telecom. Прежде, чем приступить к изучению настоящего раздела следует ознакомиться с приложениями А, Б, В и Г. В настоящем разделе приводится описание в соответствии с рекомендациями ITU-T и ETSI [49,50] процедуры аутентификации объектов аудиовизуальной службы AVSE (Audio-Visual Service Entity) ISDN с использованием шифрования с открытым ключом и электронно-цифровой подписи (ЭЦП)

сообщений, а также передача общих ключей симметричного шифрования. Объектом аудиовизуальной службы AVSE в ISDN может быть не только пользователь (оконечное оборудование), но и устройства транспортной части сети связи. Поэтому процедура аутентификации здесь применима к различным видам соединений: терминал – терминал, терминал – устройство транспортной части сети связи, два взаимодействующих устройства транспортной части сети связи. В отличие от описания аутентификации пользователя ISDN (раздел 17.4) под аутентификацией объектов AVSE понимается процедура аутентификации сообщений, которая включает проверку:

- подлинности источника сообщения;
- подлинности (целостности) сообщения, т.е. его содержимое не было изменено при доставке получателю.

В основу аутентификации объектов аудиовизуальной службы ISDN положена рекомендация ITU-T X.509 [47], в соответствии, с которой используется один или несколько уровней удостоверяющих центров (центров сертификации), создающих цепочку сертификатов. Для аутентификации объекта производится проверка подлинности открытого ключа в принятом сертификате этого объекта и проверяется подлинность электронно-цифровой подписи, используя этот открытый ключ. Одновременно с аутентификацией взаимодействующих объектов создается общий ключ для шифрования передаваемой между ними информации.

Инфраструктура систем с открытыми ключами PKI (Public Key Infrastructure) состоит из множества компонентов, среди которых пользователи, Управление сертификации, сами сертификаты и каталоги PKI предоставляет возможность структурной организации этих компонентов [10]. Одним из видов PKI является иерархия Управлений, состоящая из нескольких уровней. Процедура аутентификации объектов в указанных рекомендациях [49,50] рассматривается на примере двухуровневой иерархии - цепочки удостоверяющих центров C_X и C_Y с общим центром GCA, General Certification Authority (рис. 17.14). Реально может быть больше уровней иерархии. Названия для уровней не стандартизировано. Управление сертификации верхнего уровня (GCA) называют корневым, Центральным Управлением или доверительным якорем. Центральное Управление GCA сертифицирует управления второго уровня, которые могут обслуживать, например, страну. На рис. 17.14 это удостоверяющие центры C_X и C_Y, которые создают сертификаты соответствующих объектов X и Y. В общем случае следует иметь не одно Центральное Управление, а несколько, причем связать с каждым из них свою иерархию уровней. В современных машинах пользователей

содержатся открытые ключи более 100 Центральных Управлений (корневых уровней). В качестве каталога для хранения сертификатов предложено использовать сервер DNS.

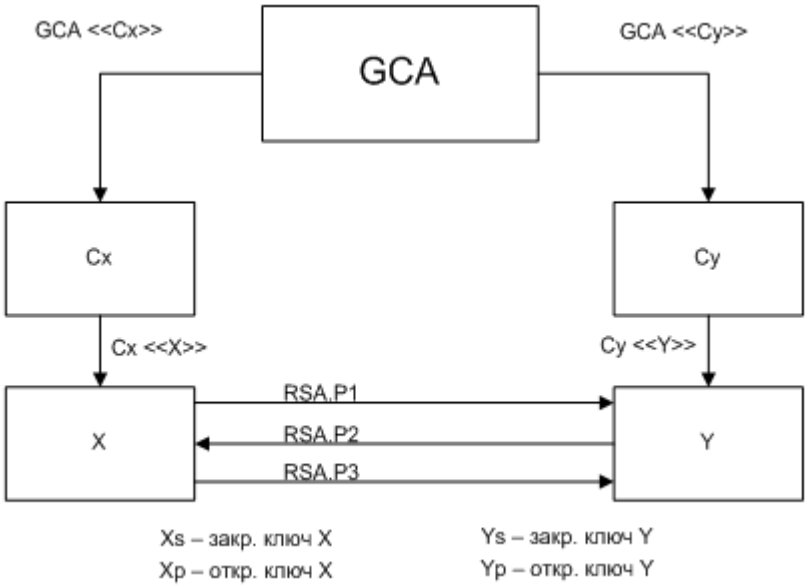


Рис. 17.14. Схема аутентификации абонентов аудиовизуальной службы ISDN и передача общих ключей симметричного шифрования

При установлении вызова процедура аутентификации использует четыре сообщения:

- RSA.P1 – инициализация аутентификации;
- RSA.P2 – ответ на запрос аутентификации;
- RSA.P3 – успешное завершение аутентификации;
- RSA.P4 – безуспешное завершение аутентификации.

Обозначим идентификатор объекта, инициирующего аутентификацию через X. Идентификатор объекта, вызываемого для проведения процедуры аутентификации, обозначим через Y. Объект X отправляет сообщения RSA.P1 и RSA.P3. Объект Y отправляет сообщение RSA.P2. Удостоверяющие центры, в которых создаются сертификаты объектов X и Y, обозначим соответственно через Cx (Cx<<X>>) и C_Y (C_Y<<Y>>). На первом шаге X отправляет объекту Y сообщение RSA.P1. Содержание сообщения RSA.P1:

GCA<<Cx>>, Cx<<X>>, Rx, Y, Xs[h(Rx, Y)]

где:

- GCA<<Cx>> - сертификат удостоверяющего центра (центра сертификации) Cx в общем удостоверяющем центре (центре сертификации) GCA;
- Rx – случайное число, сгенерированное объектом X. Rx используется для

защиты от угрозы «повтор аутентификации»;

- Xs – закрытый ключ объекта X;
- [h(Rx, Y)]- хеш-функция (Rx, Y).

Объект Y, получив сообщение RSA.P1, выполняет следующую последовательность операций.

1. Производится проверка достоверности принятого открытого ключа Xp объекта X, используя для этого принятые в сообщении два сертификаты. Сертификат центра сертификации Cx, созданный в центре сертификации GCA обозначается GCA<<Cx >>.

Этот сертификат включает следующие данные:

GCA<<Cx >>: IGCA, ICx, Cxp, T1, GCAs [h (IGCA, ICx, Cxp , T1)]

где:

- IGCA – идентификатор GCA;
- GCAs – закрытый ключ общего центра сертификации GCA;
- ICx – идентификатор центра сертификации Cx;
- Cxp– открытый ключ центра сертификации Cx;
- T1 – дата начала и окончания срока действия сертификата;
- GCAs [*] – зашифрованная информация [*] с помощью ключа GCAs,

где: [*] – хеш-функция открытой части сертификата.

Значение GCAs [*] является цифровой подписью открытой части сертификата. Для упрощения изложения материала в открытой части сертификата опущено много элементов.

Сертификат объекта аудиовизуальной службы AVSE X, созданный в центре сертификации Cx обозначается Cx <<X>>. Состав этого сертификата:

Cx <<X>>: ICx, X, Xp , T1, CXs[h(ICx, X, Xp, T1)],

где:

- ICx– идентификатор центра сертификации Cx;
- Cxs – закрытый ключ центра сертификации Cx;
- X – идентификатор объекта X;
- Xp – открытый ключ объекта X;
- T1 – даты начала и окончания срока действия сертификата;
- Cxs [*] - зашифрованная информация [*] с помощью ключа Cxs.

В объекте X записаны открытый ключ GCAp общего сертификационного центра, сертификат центра сертификации Cx - GCA<<Cx>> и сертификат объекта X (Cx<<X>>), а также

закрытый ключ объекта Xs. Сначала производится проверка достоверности открытого ключа центра сертификации Cx (т.е. Cxp). Для этого производится вычисление хеш-функции h(IGCA, ICx, Cxp , T1) открытой части сертификата этого центра сертификации Cx. Используя GCAp, производится расшифрование хеш-функции этой открытой части– GCAp [GCAs [h(IGCA, ICx, Cxp , T1)]] = h(IGCA, ICx, Cxp , T1). Открытый ключ Cxp считается достоверным, если обе хеш-функции равны. Для проверки достоверности открытого ключа Xp объекта X производится вычисление хеш-функции открытой части сертификата объекта X - h(ICx, X, Xp , T1). Используя достоверный открытый ключ Cxp производится расшифрование хеш-функции открытой части сертификата объекта X – Cxp[Cxs[h(ICx, X, Xp, T1)]] = h(ICx, X, Xp, T1). Открытый ключ Xp считается достоверным, если обе хеш-функции равны.

2. Производится проверка целостности сообщений – Rx, Y. Для этого полученная хеш-функция h(Rx,Y) сравнивается с помощью расшифрованной – Xp [Xs[h(Rx,Y)]]. Оба значения должны быть равны.

3. Производится проверка на истечение срока действия принятых сертификатов.

4. Производится проверка идентификатора объекта X, полученного в составе сертификата Cx<<X>>.

При успешном результате анализа принятого сообщения RSA.P1 объект Y отправляет объекту X сообщение RSA.P2. Содержание сообщения RSA.P2:

GCA<<C_Y>>, C_Y<<Y>>, R_Y, X, Rx, Xp[K_Y], Ys[h(R_Y, X, Rx, K_Y)]

где:

- GCA<<C_Y>> - сертификат удостоверяющего центра C_Y в общем удостоверяющем центре GCA;
- R_Y – случайное число, сгенерированное объектом Y, R_Y используется для защиты от угрозы «повтор аутентификации»;
- K_Y – случайное число, сгенерированное объектом Y, для создания ключа симметричного шифрования;
- Ys – закрытый ключ объекта Y;
- [h(R_Y, X, Rx, K_Y)] - хеш-функция (R_Y, X, Rx, K_Y).

Объект X, получив сообщение RSA.P2, выполняет следующую последовательность операций.

1.Производится проверка достоверности принятого открытого ключа Yp объекта Y, используя для этого принятые в сообщении сертификаты. Принцип работы алгоритма проверки

аналогичен описанному выше при проверке достоверности принятого открытого ключа Xp в сообщении RSA.P1.

2. Производится расшифровывание K_Y, т.е. K_Y – Xs[Xp[K_Y]].

3.Производится проверка целостности сообщений – R_Y, X, Rx, K_Y. Для этого полученная хеш-функция h(R_Y, X, Rx, K_Y) сравнивается с расшифрованной – Yp[Ys[h(R_Y, X, Rx, K_Y)]]. Оба значения должны быть равны.

4.Производится проверка на истечение срока действия принятых сертификатов.

5. Производится проверка, является ли значение Rx тем же самым, что было отправлено в сообщении RSA.P1 (защита от угрозы «повтор аутентификации»).

6. Производится проверка идентификатора объекта Y, полученного в составе сертификата Cy<<Y>>.

При успешном результате анализа принятого сообщения RSA.P2 объект X отправляет объекту Y сообщение RSA.P3 об успешном завершении аутентификации объекта Y.

Содержание сообщения RSA.P3:

R_Y, Y, Yp[K_X], Xs[h(R_Y, Y, Kx)]

где Kx – случайное число, сгенерированное объектом X, для создания общего ключа симметричного шифрования.

Объект Y, получив сообщение RSA.P3, выполняет следующую последовательность операций.

1. Производится расшифровывание Kx, т.е. Kx = Ys[Yp[Kx]].
2. Производится проверка целостности сообщений – R_Y, Y, Kx. Для этого полученная хеш-функция h(R_Y, Y, Kx) сравнивается с расшифрованной – Xp[Xs[h(R_Y, Y, Kx)]]. Оба значения должны быть равны.
3. Производится проверка, является ли значение R_Y тем же самым, что было отправлено в сообщении RSA.P3 (защита от угрозы «повтор аутентификации»).

Успешный результат анализа принятого сообщения RSA.P3 свидетельствует об успешной аутентификации объекта X объектом Y, т.е. взаимной аутентификации. Если проверка любого из сообщений RSA.P1, RSA.P2, RSA.P3 оказывается неуспешной, объект X или Y отправляют сообщение RSA.P4 об отказе в аутентификации. При этом прекращается процедура установления соединения. Рассмотрим случай одновременной передачи сообщений RSA.P1. Если объект X отправляет объекту Y сообщение:

RSA.P1 (X→Y): GCA<<Cx>>, Cx<<X>>, Rx, Y, Xs [h(Rx, Y)] и перед приемом

ответного сообщения RSA.P2 (Y→X), Y отправляет X сообщение RSA.P1 (Y→X): GCA<<C $_Y$>>, C_Y<<Y>>, R_Y, X, Ys [h(R_Y, X)], тогда объекты X и Y разрешают эту ситуацию, сравнивая Rx и R_Y.

Если Rx > R_Y, то сообщение RSA.P1 (Y→X) будет отвергнуто и Y отправляет сообщение RSA.P2.

Из значений Kx и Ky отбрасываются старшие и младшие 64 бит. Оставшиеся части Kx и K_Y складываются по модулю 2, образуя общий ключ симметричного шифрования сообщений между объектами.

Сравнивая приведенный алгоритм с протоколами IPSec и TLS (глава 13), можно заметить тот же самый принцип, что и при установлении защищенной связи.

ГЛАВА 18. IP-телефония

IP-телефония или передача голосовых данных по сетям IP (Voice over IP - VoIP) — это технология, использующая Интернет (IP-сеть) в качестве основного средства передачи данных. В отличие от сети с коммутацией каналов ТфОП/ISDN сеть Интернет, на базе которой строится VoIP, основана на коммутации пакетов. В сети VoIP, также как и в сети ТфОП/ISDN принята выделенная от транспортного потока сеть сигнализации (отличающаяся от ОКС№7). Из нескольких созданных систем сигнализации для VoIP по выполнению функций установления, управления и разъединения соединения наиболее широко используются два протокола: разработанный ITU-T протокол H.323 и протокол инициирования сеанса связи SIP (Session Initiation Protocol), разработанный инженерной группой Интернет IETF. SIP наиболее популярен у разработчиков сетей связи нового поколения NGN (Next Generaton Network) протокол [52].

Для транспортировки мультимедийных данных (аудио, видео, текст, факс) в реальном масштабе времени между участвующими в сеансе связи пользователями VoIP используется транспортный протокол реального масштаба времени RTP (Real-Time Transport Protocol) [53].

При этом следует учесть, что качество телефонной связи оператором не гарантируется. Это объясняется тем, что полоса пропускания зависит от загруженности публичной сети Интернет (данными, речью, видео и др.). Это значит, что задержки при прохождении речевых IP-пакетов определенных соединений могут быть большими. Технология VoIP рассматривается как серьезный конкурент ТфОП/ISDN, сегодня отобрала у нее примерно 20% трафика [52]. Сети IP предоставляют возможность установление следующих видов соединений.

- От телефонного аппарата к телефонному аппарату, которые подключены к ТфОП.
- От компьютера к телефонному аппарату. Мультимедийный компьютер, имеющий программное обеспечение IP-телефонии, звуковую плату (адаптер), микрофон и акустические системы, подключается к Интернету. Телефонный аппарат подключен к ТфОП.
- От компьютера к компьютеру. Оба компьютера оборудованы теми же средствами, что и в соединении от компьютера к телефонному аппарату.

18.1. Протокол SIP

18.1.1.Упрощенный пример сети на базе протокола SIP

На примере абстрактной топологи сети (рис. 18.1) покажем, как два SIP телефонных аппаратов устанавливают голосовую связь между собой. Такую упрощенную конфигурацию называют часто «SIP трапецией» [54]. Протокол SIP позволяет устанавливать не только обычные двусторонние телефонные соединения, но и (многосторонние (каждый участник может как слушать, так и говорить с собеседником), а также широковещательные (один участник говорит, а остальные могут только слушать). Во время сеанса связи могут передаваться аудио, видео или другие данные.

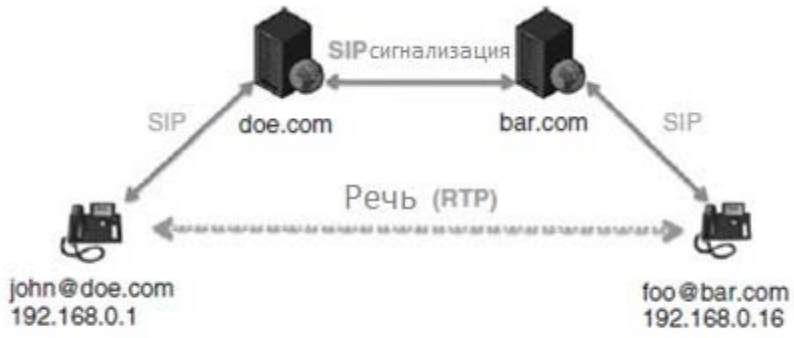


Рис. 18.1. Конфигурация сети «SIP трапеция»

Внизу рисунка показаны два SIP-телефона, которые пользователи JON и FOO используют для разговора друг с другом. Каждый телефон имеет SIP-адрес, подобный e-mail адресу, который соответствует определенному IP-адресу (на рисунке это jon@ doe.com и foo&bar.com). Первый из них соответствует IP-адресу 192.168.0.1, а второй — 192.168.0.16. Здесь jon и foo-имена пользователей, а doe.com и bar.com – имена домена. Прежде, чем начать обмениваться сообщениями, вызывающий абонент должен найти вызываемого абонента. Это задача протокола сигнализации SIP. Путь сообщений сигнализации проходит через узлы «SIP трапеции» (рис. 18.1). Каждый SIP- телефон соединяется с SIP сервером его домена, а сервера соединяются друг с другом. Левый на рисунке SIP телефон соединен с сервером, доменное имя которого doe.com, а правый – с сервером, доменное имя которого bar.com.

В сети SIP так же, как и в сети ISDN путь пакетов системы сигнализации отличается о пути медиа-потока, причем, последний короче. SIP только создает и завершает соединение (сессию), а транспорт потока данных осуществляется по алгоритму другого протокола – протокола RTP.

На примере конфигурации «SIP трапецией» приведем упрощенный цикл телефонного вызова для установления соединения. В последующих разделах приводится детализация этого процесса. SIP является протоколом сигнализации, т.е. также, как ОКС№7 в ТфОП/ISDN выполняет функцию установления, управления и разъединения соединения. На рисунке 18.2 показан упрощенный цикл телефонного вызова абонентом. Предварительно оба абонента заявляют о себе своим серверам, т.е. регистрируются. Это осуществляется отправлением запроса REGISTER (#1a и #1b на рисунке). SIP сервера отправляют положительные подтверждения на запросы, используя ответы «200 ОК». В результате регистрируется местоположение этих SIP телефонов. Затем, когда в сообщении #3 пользователь с адресом john&doe.com набирает адрес foo&bar.com, в его сервер домена отправляется запрос на установление соединения. В терминах SIP этот запрос называется ”INVITE”. Он включает информацию кто и кого вызывает, характеристики телефонных аппаратов и другую полезную информацию. Сообщение через сервера передается вызываемому абоненту. Сервер doe.com определяет, что адрес назначения находится в другом домене (bar.com) и направляет туда запрос INVITE (сообщение #4). Сервер с доменным именем bar.com, используя информацию регистрации, направляет этот запрос (сообщение #4) на SIP телефон назначения (с адресом foo&bar.com). Каждый транзит (хоп) подтверждает прием запроса INVITE, отправляя сообщение ”100 trying” (#5, #7 и #8). В том случае, если подтверждение не получено, отправитель будет повторять передачу запроса INVITE. Установка вызова завершается в приведенном примере, когда вызываемый участник отвечает на вызов звуковым сигналом (“180 ringing”) извещения о поступлении к нему вызова (#9, #10 и #11). Затем вызываемый телефон выбирает кодеки для сжатия речи и отправляет окончательный положительный ответ “200 OK” вызывающему абоненту (#12). Эти сообщения далее проходят по тому же пути (#13, #14) и для надежности подтвеждаются (#15, #16, #17). Теперь соединение (сеанс) установлено и оба телефона начинают обмениваться пакетизированной речью, используя протокол RTP. Когда любой из участников сессии решает повесить трубку, он отправляет запрос BYE. Запрос BYE следует по тому же пути, что и при вызове (#18, #19, #20). На этом сеанс завершается. Окончание сеанса здесь инициируется с телефона foo&bar.com. Рассмотренная конфигурация сети на базе протокола является упрощенной только для общего описания принципов сети SIP и не позволяет описать все

основные функции этой сети. К ним, в частности, относятся протоколы маршрутизации, учитывающие более сложные конфигурации сети, мобильность пользователя (т.е. способность получать доступ в любом месте), обеспечение информационной безопасности в сети и др.

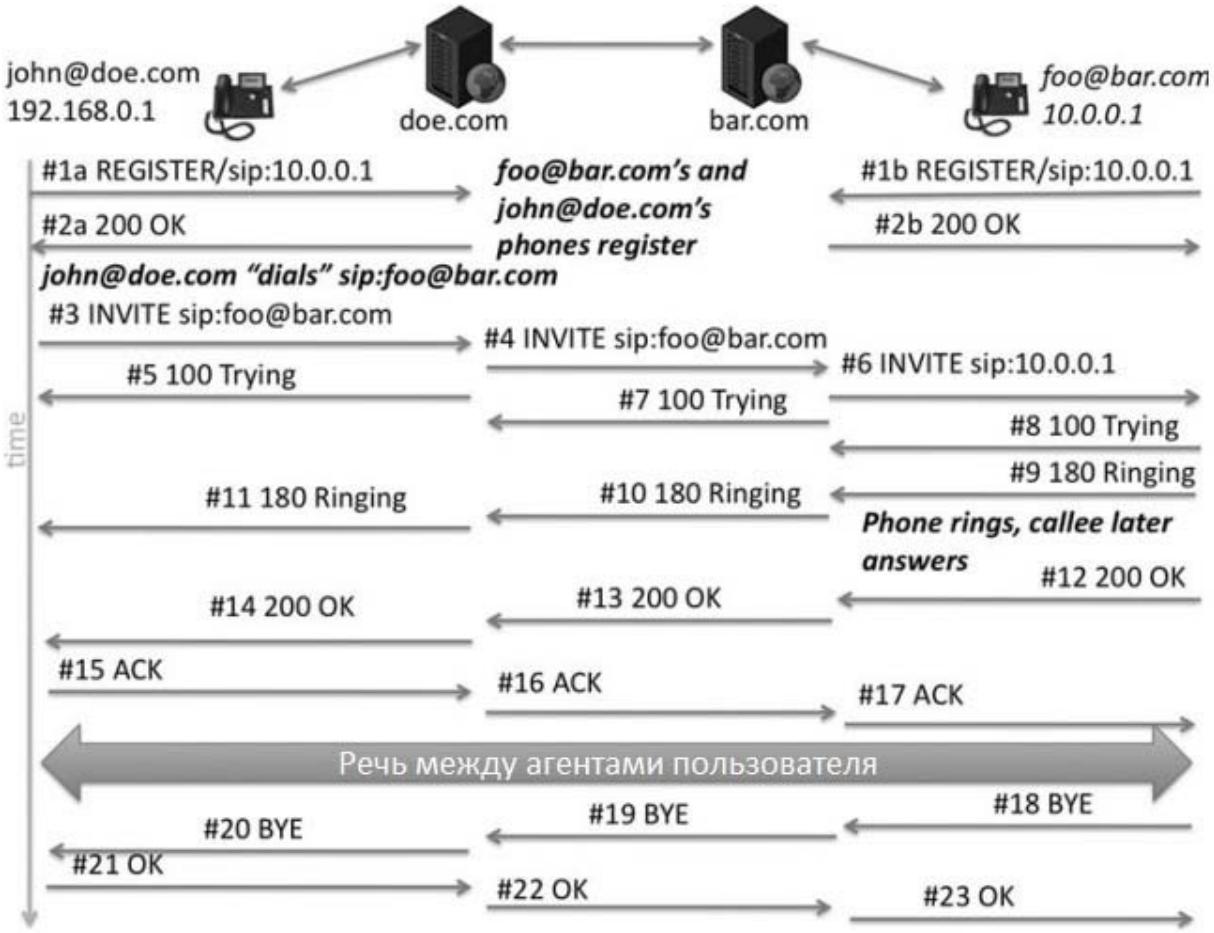


Рис. 18.2. Цикл телефонного вызова абонентом при конфигурации сети рис. 18.1

18.1.2. Сетевые компоненты протокола SIP

Сеть SIP содержит следующие основные стандартизированные SIP устройства: SIP агент пользователя, SIP прокси-сервер, SIP сервер переадресации, SIP регистратор, взаимный агент пользователя.

Агент пользователя UA (User Agent). UA является одноранговым (peer-to-peer) элементом, способным инициировать SIP запрос и принимать их. Часть программного обеспечения

агента UA, которая создает новые запросы (например, нажатием кнопок на SIP-телефоне), отправляет их и обрабатывает принятые ответы называется клиентом агента пользователя UAC (User Agent Client). Другим примером UAC является перенаправление SIP запроса прокси-сервера от имени UAC. Другая часть программного обеспечения агента UA, которая принимает запросы, обрабатывает их и генерирует ответы, основываясь на действиях пользователя, полученных сообщениях и других событиях, называется сервером агента пользователя UAS (User Agent Client).

UAC и UAS выполняют соответственно функции запроса и ответа, что во многом похоже на принцип “клиент-сервер” протокола HTTP (при котором клиент посылает через сеть запрос серверу, сервер выполняет определенные действия или ищет запрашиваемые данные и затем отсылает ответ клиенту). SIP протокол выполняет транзакцию, которая состоит из запроса к серверу, обработки его сервером и окончательным ответом от сервера. В некоторых случаях сервер может отправить несколько ответов прежде, чем отправить окончательный ответ.

Прокси-сервер (Proxy). Прокси-сервер является промежуточным узлом, который выполняет функцию маршрутизации. Он маршрутизирует SIP-запросы к UAS и SIP-ответы к UAC. На пути к UAS запрос может проходить несколько прокси-серверов. Прокси-сервер действует от имени других клиентов и содержит функции клиента (UAC) и сервера (UAS). Прокси-сервер выполняет также следующие функции:

аутентификацию, т.е. проверку подлинности источника SIP-запроса;

авторизацию, т.е. проверку на право обработки данного запроса в соответствии с принятой политикой

и др.

Сервер переадресации (redirect server). Сервер переадресации предлагает соединиться с UAC по другому адресу (по причине переезда или с целью балансирования нагрузки). Сервер переадресации в отличие от прокси-сервера после получения адреса вызывающей стороны не передает запрос INVITE в оборудование вызываемого пользователя. Сервер переадресации передает этот адрес вызывающей стороне. Оборудование вызывающей стороны завершает транзакцию с сервером переадресации запросом ACK. Затем оборудование вызывающего пользователя передает запрос INVITE на адрес, полученный от сервера переадресации.

Регистратор (registrar) или сервер регистрации. Прежде, чем перейти к функции регистратора рассмотрим принятую адресацию в SIP. Адреса SIP пользователя или ресурса является глобальным маршрутируемым адресом, по которому может находиться

пользователь. Постоянные адреса SIP пользователя или ресурса называют записью обращения к адресу AoR (Adress of Record). Эти адреса подобны адресу электронной почты. В качестве адресов пользователей используются специальные универсальные указатели ресурсов — Адреса SIP обычно называют SIP URI (Universal Resource Identifier, единообразный идентификатор ресурсов). Приняты следующие форматы SIP URI:

sip:имя пользователя&домен, sip:имя пользователя&хост.

sip:имя пользователя&IP-адрес, номер телефона&шлюз.

Если указывается доменное (символьное) имя, то с помощью службы (сервера) доменных имен DNS (Domain Name Service) определяется IP-адрес.

Поле пользователя указывется либо по имени, либо по номеру телефона. Если указывается телефонный номер в соответствии со стандартом ITU-T E.164, то с помощью службы (сервера) ENUM (Elephone Number Mapping) производится преобразование в IP-адрес и наоборот. Такая необходимость возникает при использовании обычного стационарного телефонного аппарата в сети SIP. Адресация такого аппарата осуществляется по протоколу ITU-T E.164 и включает код страны (CC), национальный код места назначения (NDC), номер абонента (SN).

Ниже приведем примеры адресов SIP URI:

sip:bob&bmstu.ru (пользователь идентифицирован по имени)

sip:3414576& proxy1.bmstu.ru (пользователь идентифицирован по номеру телефона)

В протоколе SIP также используют идентификаторы SIPS URI (SIP Secured URI), указывающие на потребность в защите сквозной сигнальной информации в сети. Вопросы обеспечения ИБ в сети SIP рассматриваются ниже в настоящей главе.

Приведенный на рис. 18.1 и 18.2 пример не учитывает возможность мобильности пользователя. Пользователь может перемещаться в пределах сети, поэтому для установления сеанса необходимо знать адрес его местоположения на текущий момент. Для этого пользователь сохраняет постоянные SIP адреса, называемые AoR. Связь между адресом AoR и текущим местоположением пользователя хранится в базе данных сервера регистрации (registrar). Пользователь информирует свой новый адрес в этот регистр с помощью специального сообщения. Пример такой регистрации приводится ниже в разделе 18.1.3.1. Если пользователь желает установить соединение с другим пользователем, необходимо определить адрес узла, по которому доступен адресат. Прокси-серверы и серверы перенаправления позволяют определить этот адрес, обратившись к серверу регистрации.

Для предоставления этой информации сервер использует базу данных, в которой каждому запрошенному адресу поставлено в соответствие один или несколько адресов, связанных с вызываемым пользователем. С помощью сервера-регистратора протокол SIP обеспечивает непосредственно агенту изменение в базе данных сервера для определения местоположения. Осуществляется это с помощью запроса REGISTER. Если пользователь провел регистрацию с определенным сервером регистрации, то эта информация будет впоследствии использована прокси-сервером этого домена для маршрутизации к терминалу этого пользователя. Когда пользователь передает запрос REGISTER, он может предложить срок действия этой регистрации.

Взаимный агент пользователя (Back-to-Back User Agent – B2BUA). Прокси-сервер является пассивным элементом, осуществляя только ретрансляцию SIP сообщений, вводя в них лишь незначительную модификацию. Это недостаточно, так как иногда требуется управление вызовами со стороны сети. В отличие от прокси-сервера, сервер B2BUA может инициировать новые вызовы SIP, а также изменять и завершать существующие вызовы.

Приведенные серверы на рис. 18.1 выполняют упрощенную функцию прокси-сервера. Дополнительной функцией прокси-сервера в реальной конфигурации сети является установление местонахождении клиента с помощью сервера определения местоположения. В этом случае прокси-сервер после принятия им запроса INVITE от вызывающего пользователя устанавливает местонахождение клиента (т.е. адрес вызывающей стороны) с помощью сервера определения местонахождения. Затем прокси-сервер передает запрос INVITE в оборудование вызываемого пользователя.

18.1.3. Сообщения SIP

Из приведенного примера видно, что сообщения SIP делятся на запросы и ответы.

Запросы SIP

Запросы SIP (SIP request) – это сообщения, которые передаются от клиента серверу, чтобы он осуществил операцию SIP. В примерах были показаны запросы:

- INVITE (приглашение на установление сеанса);
- ACK (подтверждение, что клиент агента пользователя UAC получил окончательный ответ на запрос INVITE;
- REGISTER (регистрация клиентом информации о его текущем месторасположения в соответствии с записями AoR пользователя на сервере SIP;
- BYE (агент UA завершает установленный ранее сеанс).

Позже будут рассмотрены еще два типаа запросов.

- CANCEL (позволяет пользовательским агентам и сетевым серверам отменить ранее переданный запрос, если ответ на него еще не получен);
- OPTION (позволяет получить информацию о функциональных возможностях пользовательских агентов и сетевых серверов).

Сервер посылает клиенту ответ SIP для того, чтобы оповестить его о состоянии запроса SIP, посланного клиентом на сервер раньше.

Ответы SIP

Агенты UAC и прокси-серверы создают ответы SIP на запросы SIP для того, чтобы инициировать агент UAC. Ответы SIP пронумерованы от 100 до 699 и сгруппированы как 1xx, 2xx и так далее до 6xx. По классификации они разделены на предварительные и окончательные. Предварительный ответ означает, что сервер работает, но это неокончательный ответ. Из приведенного примера к таким ответам относятся: 100 trying, 180 ringing. Завершение обработки и финальное состояние запроса SIP означает окончательный ответ. Все ответы остальных классов являются окончательными. Из приведенного примера таким ответом является “200 OK”.

18.1.3.1. Поля заголовка сообщения при регистрации SIP

Настоящий раздел посвящен описанию состава сообщений SIP на примере

регистрации SIP и принципа мобильности пользователя.

Каждое сообщение SIP состоит из трех полей: *начальная строка, заголовок сообщения и тело сообщения.*

На рис. 18.3. показан пример содержания сообщений для простой транзакции: запрос REGISTER и положительный ответ на него. Как правило, функции сервера регистрации и прокси-сервера выполняет тот же сервер. Агент пользователя UA посылает запрос REGISTER на сервер регистрации домена, представляя свой текущий адрес в поле заголовка Contact. Постоянный адрес SIP пользователя AoR содержится в поле *To* запроса. Сервер регистрации модифицирует базу данных расположения служб, чтобы привязать постоянный адрес пользователя к его текущему адресу.

Структура сообщения запрос REGISTER
REGISTER sip:iptel.org;transport=udp
From: “Jiri”@iptel.org>
To: : “Jiri”@iptel.org>
Cseq: 119065 REGISTER
Contact:<sip:jiri@192.168.1.101>;expires=3600

Структура сообщения ответ REGISTER
200 OK
From: “Jiri”@iptel.org>
To: “Jiri”@iptel.org>
Cseq: 119065 REGISTER
Contact:<sip:jiri@192.168.1.101>;expires=3600

Рис. 18.3. Сообщения транзакции: запрос REGISTER и положительный ответ на него

Начальная строка

В поле начальной строки *запроса* определена цель сообщения. При этом указывается идентификатор тип запроса и адрес назначения в форме URI. На рис. 18.3 это REGISTER и имя домена назначения iptel.org. Обращаясь к серверу регистрации, пользователь указывает

адрес, по которому он находится в настоящее время. Адресом URI в начальной строке, sip:iptel.org;transport=udp, служит для маршрутизации с целью выполнения запроса REGISTER. В качестве транспортных протоколов модели TCP/IP могут использоваться протоколы UDP или TCP. В данном случае используется транспортный протокол UDP. Этот дейтаграммный протокол не устанавливает соединение на транспортном уровня. Надежная передача обеспечивается повтором запроса.

При прохождении запроса через несколько серверов SIP может потребоваться изменение маршрутизации или услуги, что в свою очередь может потребовать изменение адреса назначения. Например, к пользователю потребуется направить запрос по IP-адресу. Тогда URI изменяется на sip:juri@10.0.0.1; transport=tcp. В данном случае используется транспортный протокол TCP, устанавливающий соединение. Начальная строка *ответа* является строкой состояния и указывает на результат в цифровой и текстовой форме. В этом примере 200 ОК.

Заголовок сообщения

Следующее поле после начальной строки (заголовок сообщения) состоит из полей, которые осуществляют передачу сигналов и несут информацию о маршрутизации для объектов сети SIP. В базовом протоколе SIP предусмотрено около 50 полей заголовков, выполняющих различные функции. Каждое поле заголовка состоит из имени поля и значения поля. Приведем краткое описание функций некоторых полей заголовка SIP.

- *To*: идентификатор получателя запроса. Это поле содержит адрес AoR получателя запроса.
- *From*: идентификатор отправителя запроса. Это поле содержит адрес AoR отправителя запроса.

Часто недостаточно адреса SIP в поле *From*, особенно в случаях, когда вызовы SIP оканчиваются в ТфОП. При этом оборудование не может идентификатор вызывающего пользователя идентифицировать в нецифровой форме. В таком случае прокси-сервер добавляет к полю *From* поле заголовка *P-Asserted-Identity* телефонный номер отправителя, как показано на рис. 18.4.

From: “John doe” joe@ipel.org; tag=9texf/

P-Asserted-identity:<tel:16181234567>

Рис. 18.4. Поле заголовка *From* в комбинации с заголовком *P-Asserted-Identity*

С точки зрения информационной безопасности оба заголовка From и P-Asserted-Identity могут быть легко изменены злоумышленником, так как уязвимы угрозе «человек посередине». В качестве защиты может быть использован протокол безопасности на транспортном уровне TLS (глава 13).

Для того, чтобы быть уверенным в том, что источник запроса является тот, за кого он себя выдает SIP использует протокол аутентификации, основанный на разделении пароля между сервером и клиентом. Детали этого протокола изложены ниже.

- *Contact*: описывает местонахождение клиента. Это особенно важно для запроса пользователя REGISTER. В поле *Contact* этого запроса содержится текущий (контактный) адрес SIP телефона, который должен быть связан с постоянным (глобальным) адресом AoR. Это поле заголовка имеет параметр *expires*, который указывает на период времени эта привязка допустима. На рис. 18.3 для параметра *expire* установлено значение 3600 секунд. Для сохранения этой привязки агент UA периодически посылает сообщения регистрации, чтобы обновлять эту информацию. Такой механизм регистрации контактного адреса на сервере регистрации позволяет протоколу SIP поддерживать мобильность пользователя. Когда агент UA посылает запрос REGISTER серверу регистрации SIP он уведомляет службу расположения о своем текущем адресе. Теперь прокси-сервер может передавать запросы этому мобильному пользователю на основании контактного адреса в базе данных сервера местоположения.

- *CSeq*: целочисленное значение последовательности запросов и названия запроса (в примере REGISTER). Это поле служит для защиты от потери сообщений или повторной их передачи.

- *Via:* поле заголовка в каждом прокси-сервере содержит список элементов сети SIP, через которые запрос прошел. Список нужен для тех случаев, когда необходимо, чтобы запросы и ответы проходили по одному и тому же пути.

- *Record-Route*: поле заголовка Record-Route используется для того, чтобы запомнить путь инициализирующего запроса на пути от UAC до UAS. Все прокси-сервера добавляют эти поля для того, чтобы следующие запросы в процессе диалога маршрутизировались через эти же прокси-серверы.

- *Rout:* поле заголовка служит для принудительной маршрутизации запроса в соответствии со списком прокси-серверов.

- *Loop detection* (обнаружение петли). Каждый SIP запрос должен включать счетчик, который указывает сколько «хопов» может еще пройти. Этот счетчик называется *Max-Forwards* и напоминает “Время жизни“ в заголовке IP-пакета. Первоначальное значение устанавливается клиентом. Это число уменьшается каждым сервером, который пересылает запрос далее.
- *User-Agent* и *Warning*. Поле заголовка User-Agent содержит ограниченную информацию о клиенте, инициирующем запрос. Поле заголовка Warning содержит дополнительную информацию, об инициаторе ответа.
- *Proprietary extention (частные расширения).* Некоторые производители считают полезным расширение некоторых возможностей, но не переносят на них стандартизацию. В качестве примера может быть использовано оборудование, фиксирующее характеристик качество обслуживания QoS по завершению вызова.

Тело сообщения

Тело сообщения приведем на примере запроса INVITE. Эта часть заголовка сообщения служит для выполнения функции обмена определенными данными между двумя участниками сессии. В соответствии с протоколом описания сессии (сеанса) SDP (Session Description Protocol), в простейшем случае в тело заголовка включены IP-адреса и номера портов, по которым агенты пользователя обмениваются данными.

Протокол SDP, определенный в RFC 2327, описывает содержимое сессий, включая телефонию, приложения мультимедиа. SDP содержит также следующую информацию.

Медиа потоки: сессия может реализовывать несколько потоков данных. В протоколе SDP в настоящее время определены аудио, видео, данные, управление и приложения, сходные с MIME типами электронной почты в Интернете.

Адреса: SDP указывает адреса места назначения для медиа потоков при многоадресной (multicusting) передаче.

Порты: для каждого потока специфицируются номера UDP портов для отправителя и получателя.

Время старта и остановки: Эти данные используются в случае широковещательных сессий, например, телевизионных или радио программ. Указываются время начала, завершения и времена повторов сессии.

Документ RFC 3264 предоставляет модель согласования на основе механизма

предложения/отклика, в которой партнеры обмениваются SDP сообщениями с целью достичь согласия относительно данных, подлежащих пересылке. Примером информации в поле тела сообщения может быть, например, выбор кодека при использовании телефонии.

Как показано ниже (в подразделе 18.1.4) в протоколе SIP для телефонии (SIP-T) предусмотрено инкапсулирование в тело запроса INVITE и ответов сообщений ОКС№7 прикладного уровня ISUP.

18.1.3.2. Транзакции и диалоги SIP

SIP – это протокол ориентированный на транзакции: взаимодействие между элементами сети происходит путем обмена сообщениями. Транзакция SIP осуществляется между агентами UAC и UAS. Она включает все промежуточные серверы SIP и состоит из всех сообщений запросов и ответов, начиная с INVITE и кончая окончательным ответом агента UAS. Транзакция SIP может установить, изменить или завершить мультимедийный сеанс. Одна транзакция состоит из запроса и нескольких ответов на него. Из приведенного примера на рис. 18.2 видно, что в транзакцию запроса INVITE входит еще один запрос ACK. Процедура транзакции запроса INVITE сложнее, чем процедуры транзакций других запросов. Примером может быть возможность отменять транзакцию после переданного запроса, если ответ на него еще не получен. Для этого необходимо отправить запрос CANCEL. Другим примером является возможность разветвления прокси-сервером запроса INVITE на несколько пунктов назначения.

Транзакция SIP может привести к установлению, изменению или завершению мультимедийного сеанса. На одном установленном сеансе может осуществляться несколько определенных транзакций. Такое состояние отношений между двумя или несколькими агентами UA называется диалогом. Транзакции SIP используют протоколы транспортного уровня TCP и UDP. При использовании протокола UDP приложение SIP запускает таймер для повторения запроса и гарантии сквозной надежности.

18.1.3.3. Маршрутизация сообщений SIP

Основная функция прокси-сервера является маршрутизация. Для маршрутизации сообщения поле заголовка сообщения INVITE содержит запись адреса AoR SIP вызываемого пользователя. Прокси-сервер использует этот адрес для поиска адреса получателя. Запрос может пройти через несколько прокси-серверов прежде, чем достигнет агента назначения

UAC. Каждый прокси-сервер на пути следования должен принимать решение о маршрутизации. Прокси-сервер может перезаписать URI запроса и добавить в заголовок поле *Via*. Ответы SIP проходят через тот же набор прокси-серверов, что и запрос, но в обратном направлении. Прокси-сервер обычно выполняет функцию сервера регистрации. Таким образом, прокси-сервер имеет доступ к базе данных расположения пользователя назначения, которая создается при регистрации этого пользователя. Если в строке запрос указан прокси-сервер, несущий ответственность за домен, он осуществляет поиск в базе данных. В результате поиска могут быть получены адреса, по которым находится вызываемый пользователь. В результате север SIP, прежде всего, выполняет функцию маршрутизации, т.е. определяет устройство следующей транзитной точки, на которое следует переслать сообщение SIP. Ближайшая точка перехода может быть другим прокси-сервером, сервером переадресации, шлюзом ТфОП или оконечным агентом UAC.

18.1.4. Протокол SIP-T

Звонки в SIP-телефонии можно совершать с компьютера или специального SIP-телефона, непосредственно подключенных к сети Интернет, либо с обычного телефона (через набор индивидуального пин-кода доступа), подключенного к Интернет через ТфОП. Разработан стандарт RFC 3372 [55] (с переводом в работе [56]) по установлению соединений стационарных аппаратов через сеть SIP. Такие протоколы получили название SIP-T (SIP extention for Telepfony, распространение SIP для телефонии). Кратко изложим некоторые положения этого стандарта.

На рис. 18.5 приведена схема прохождения сообщений сигнализации при установлении соединений между абонентами сети ТфОП. Она включает:

- участки ОКС№7 между граничными станциями ТфОП/ISDN и шлюзами сигнализации MGC (Media Gateway Controller) - MGC1 и MGC2. При этом имеется в виду сообщения всех четырех уровней системы ОКС№7. Шлюзы производят преобразование сигнальных сообщений протоколов ОКС№7 в сигнальные сообщения протокола SIP и наоборот. Шлюз MGC называют также Softswitch, преобразователем систем сигнализации. Со стороны сети SIP он является клиентом агента пользователя UAC.

- сеть SIP.

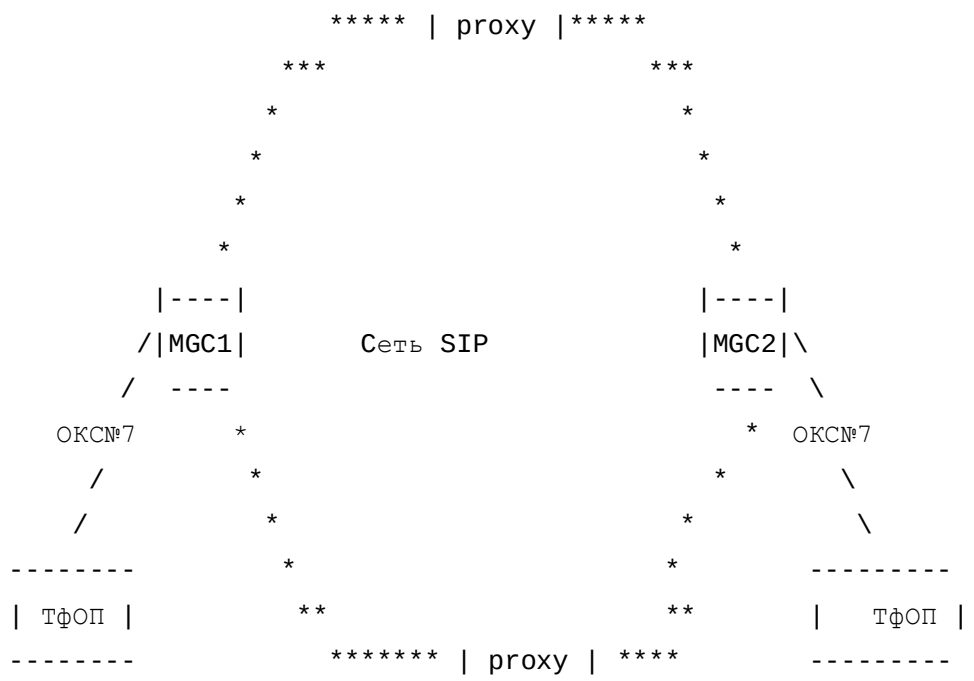


Рис. 18.5. Структура транзитной связи сигнализации через сеть SIP при установлении/разъединении соединений между абонентами сети ТфОП через сеть SIP

Требования по взаимодействию систем сигнализации и функции протокола SIP-T изложены в стандарте RFC 3372 (табл. 18.1).

Таблица 18.1. Требования по взаимодействию систем сигнализации и функции протокола SIP-T

Требования по взаимодействию ОКС№7- SIP	Функции SIP-T
Прозрачность сети SIP для сигнализации ISUP	Инкапсуляция ISUP в тело запросов SIP
Маршрутизация сообщений SIP по информации в ISUP	Трансляция информации из ISUP в заголовок запросов SIP
Передача дополнительной сигнальной информации ISUP во время сеанса связи (например, перенос информации об остатке на счете – биллинговой информации)	Использование запроса SIP - INFO

На рис. 18.6 показана упрощенная диаграмма примера обмена сообщениями сигнализации (прикладного уровня ОКС№7, запросы и ответы SIP). Она соответствует приведенной выше

на рис. структуры транзитной связи при установлении соединения.

Рис.18.6. Диаграмма примера обмена сообщениями сигнализации

Сообщения ОКС№7 соответствуют прикладному уровню ISUP (см. рис.17.7, глава 17). В шлюзе MGC1 сообщение ОКС№7 IAM инкапсулируется в тело запроса INVITE. Кроме этого из IAM в заголовок INVITE переносятся:

в поле *From* – адрес вызываемого абонента;

в поле *To*– адрес вызывающего абонента.

18.2. Информационная безопасность SIP

18.2.1. Угрозы ИБ

В настоящем разделе приводятся изложенные в стандарте RFC 3261 [57] примеры некоторых угроз ИБ в сетях SIP. Эти угрозы являются общими для большинства сетей SIP.

18.2.1.1. Угрозы с использованием регистрации

Регистрация может производится не только самим пользователем терминала, но и нарушителем. В этом случае в заголовках *From* и *To* запроса REGISTER установлены одинаковые адреса. Злоумышленник может пожелать, чтобы соединения других пользователей устанавливались с ним. Для этого он перерегистрирует всех легитимных пользователей, а затем регистрирует свое устройство. В результате при отсутствии защиты, гарантирующего подлинность источника требования SIP, вызовы от других пользователей поступают злоумышленнику. Этот пример показывает необходимость аутентификации источника запроса SIP.

18.2.1.2. Подмена сервера

Имя домена, к которому должен поступить запрос SIP установлен в поле Request-URI заголовка запроса. UAC в этом домене связан непосредственно с сервером, которому передает запрос. Возможна угроза ИБ путем подмены легитимного сервера. В результате фиктивный сервер переправляет запрос на другой домен. При регистрации пользователя все запросы к нему будут направляться в ложный сервер. Этот пример показывает необходимость защиты с помощью механизма аутентификации сервера (т.е. взаимная аутентификация).

18.2.1.3. Изменение содержания тела заголовка

В сети SIP требуется обеспечить конфиденциальность некоторых данных в сообщениях сигнализации. Это относится, например, к инкапсулированным данным ОКС№7 в тело заголовка. Это требование вызвано угрозой злоумышленно изменить тело заголовка с целью прослушивания переговоров по установленному соединению. Этот пример показывает необходимость предоставить возможность шифрования/дешифрования некоторых данных тела заголовка, целостность и аутентификацию.

18.2.1.4. Прерывание сеанса связи

После установления соединения последующие запросы могут быть отправлены для

изменения состояния диалога и/или сеанса. Важно, чтобы пользователи были уверены в том, что эти запросы не подделаны злоумышленниками. Злоумышленник может узнать некоторые параметры во время первоначального установления сеанса (поля заголовка *To, From* и др.), а затем передать ложный запрос INVITE. Последний запрос видоизменяет сеанс (например, переправляет медиапотоки для атаки прослушивания разговоров). Этот пример, также как и предыдущий, показывает необходимость предоставить возможность шифрования/дешифрования некоторых данных, обеспечения их целостности и аутентификации.

18.2.1.5. Отказ в обслуживании

Атака отказ в обслуживании (DoS) нацелена на перевод сетевого элемента в состояние неработоспособности (неготовности). R таким угрозам и обычно относят направление чрезмерно большого трафика на его интерфейсы. Распределенная DDoS (Distributed Denial of Service) атака позволяет одному пользователю сети SIP воздействовать на много сетевых узлов с тем, чтобы они передавали очень большой сетевой трафик на определенный узел сети («затопили» его). Во многих архитектурах прокси-серверы сети SIP взаимодействуют с публичной сетью Интернет, к которой подключено множество IP-терминалов. В результате, сеть SIP предоставляет возможность для DDoS атак, что должно быть учтено разработчиками и операторами сетей SIP.

Злоумышленники могут создавать поддельные запросы, содержащие фальсифицированные IP-адреса источника и соответствующее поле заголовка Via. Эти параметры идентифицируют ложный источник этих запросов, на который затем через агента пользователя или прокси-сервер SIP генерируется трафик, приводящий к DoS.

Аналогично злоумышленник может использовать фальсифицированные значения заголовка Route. Этот заголовок служит для принудительной маршрутизации запроса в соответствии со списком прокси-серверов. Фальсифицированные значения в составе этого заголовка поступают на прокси-серверы. Далее запросы размножаются и увеличенный поток поступает по указанному адресу. Возможность создания злоумышленником таких атак DoS имеет место, если при запросе регистрации сервер регистрации не производит достаточно надежную аутентификацию пользователя. Использование многоадресной (multicusting) передачи запросов также может предоставить злоумышленнику возможность в создании таких атак DoS.

Другая причина атаки DoS может иметь место в сети SIP-T, когда на участке сети связи

ТфОП/ISDN злоумышленником отправляются ложные сообщения управления сетью сигнализацией подсистемы ОКС№7. К числу таких сообщений относятся сообщение о полной перегрузке (сообщение управление переносом - TFC, Transfer control) и сообщение об ограниченной перегрузке (TFR, Transfer restricted). Эти сообщения направляются в адрес шлюза сигнализации MGC и приводят к нарушению маршрутизации. Результатом является полное или частичное прекращение возможности установления сеанса связи через указанные в этих сообщениях пункты сигнализации. Указанные два ложных сообщения в адрес MGC являются не единственными, которые могут привести к таким последствиям. К таким сообщениям относятся также и другие, выполняющие функции управления сетью сигнализации ОКС№7, которые подлежат рассмотрению ниже в главах 19 и 22:

- функция MTP вынужденная ремаршрутизация (сообщение TFP);
- функция MTP управление потоком сигнального трафика подсистемы MTP3 (сообщение UPU);
- функция MTP управляемая маршрутизация (сообщение TFA);
- функция перезапуск MTP;
- функция MTP перевод трафика на резервное звено сигнализации (сообщение COO);
- функция MTP восстановление трафика на исходное звено сигнализации сообщение (COA).

18.2.2. Требования к способам обеспечения ИБ в сети SIP

В настоящем разделе приводятся изложенные в стандарте RFC 3261 [57] основные требования к способам обеспечения ИБ в сетях SIP. Эти требования сводятся к следующим способам ИБ сигнальных сообщений.

- **Конфиденциальность сообщений.** Запросы и ответы SIP содержат информацию, которая в открытом виде по сети SIP передаваться не должна. Следует учесть, что невозможно обеспечить сквозное шифрование всего заголовка сообщения SIP из конца в конец, так как в них содержатся необходимые для маршрутизации поля адресации (Rout, Request-URI, Via). Передача этих данных в открытом виде представляет так же, как и в примере шифрования в сети передачи данных (глава 2, раздел 5) угрозу анализа трафика. Поэтому должно производиться канальное шифрование/дешифрование, т.е. между ретрансляторами (hop-by-hop). Обратите внимание на отличие от канального шифрования в сети передачи данных в главе 2,

которое вызвано различием архитектур выполнения функций сигнализации. В сети SIP используется выделенная сеть сигнализации. Поэтому ИБ рассматривается отдельно для сети сигнализации и для медиапотока. В сети SIP некоторые поля адресации изменяются в транзитных пунктах прокси-серверов, а в приведенном примере сети передачи данных адрес пункта назначения остается неизменным. Тело сообщения SIP может быть зашифровано из конца в конец. В составе тела сообщения с помощью цифрового конверта может быть передан общий ключ шифрования сеанса связи (глава 13).

- Аутентификация участников сеанса. Должна быть проверена подлинность взаимодействующих пользователей сеанса связи и прокси-серверов. Для SDP-тела требуется отдельный механизм взаимной аутентификации.
- Целостность сообщений.
- Защита от атак повтора сообщений.
- Защита от атак фальсификации сообщений.
- Защита от атак DoS.

Отдельного внимания требует обеспечение конфиденциальности, целостности и аутентификация данных в составе тела заголовков сообщений SIP, требующее сквозного обеспечения информационной безопасности между пользователями сеанса связи.

Все механизмы обеспечения ИБ сети SIP в соответствии со стандартом RFC 3261 можно разделить на средства, базирующиеся на протоколы ИБ прикладного, транспортного и сетевого уровней IP-сети.

К таким протоколам прикладного уровня, протоколы ИБ которых используются для защиты от угроз в IP-сети, относятся:

- протокол аутентификации при передаче гипертекста HTTP (Hypertext Transfer Protocol);
- протокол ИБ электронной почты S/MIME (Security/Multipurpouse Internet Mail Extention, стандарты RFC 2632-2634). Этот протокол используется в сети SIP в соответствии с положениями последней версии стандарта по SIP RFC 3261;
- протокол ИБ электронной почты PGP, описание которого приведено в главе 13. Этот протокол использовался в сети SIP в соответствии с положениями предыдущей версии стандарта по SIP (RFC 2543 [58]).

В главе 13 приведено описание протоколов ИБ сетевого уровня IPSec и протокола ИБ транспортного уровня TLS.

18.2.3. Механизмы обеспечения ИБ

18.2.3.1. Механизм ИБ SIP-сети на базе протокола IPSec

В предыдущей версии стандарта по SIP (RFC 2543) в качестве механизма ИБ протокол IPSec рассматривается:

- для шифрования на каждом канальном участке сети SIP (hop-to-hop);
- аутентификации заголовка (обеспечивая при этом его целостность и контроль доступа).

В последней версии стандарта по SIP (RFC 3261) протокол IPSec рассматривается как возможный вариант обеспечения ИБ:

- для сети SIP в качестве дополнительного средства защиты прикладного уровня хостов;
- для сервера агента пользователя UAS и взаимодействующего с ним первого ретранслирующего с ним прокси-сервера;
- для обеспечения ИБ на каждом канальном участке сети SIP (hop-to-hop).

18.2.3.2. Механизм ИБ SIP-сети на базе протокола TLS

Протокол TLS обеспечивает аутентификацию, целостность сообщений и шифрование. В соответствии с требованиями стандарта RFC 3261 прокси-серверы, серверы перенаправления и регистрации должны реализовывать протокол TLS и обеспечивать взаимную и одностороннюю аутентификацию. Строго рекомендуется, чтобы UAS могли также действовать как серверы TLS. Прокси-серверы, серверы перенаправления и регистрации должны содержать сертификаты своего хоста. Серверы агента пользователя могут иметь собственные сертификаты для взаимной аутентификации по протоколу TLS. Все элементы сети SIP, которые используют протокол TLS, должны иметь механизм для проверки достоверности сертификатов, полученных при обмене по протоколу TLS. Для этого необходимо обладать одним или несколькими корневыми сертификатами (предпочтительно одним или несколькими хорошо известными распределителями сертификационных сайтов, сравнимых с теми распределителями, которые выпускают корневые сертификаты для веб-браузеров).

В стандарте RFC 3261 отмечается, что протокол TLS наиболее пригоден для

архитектуры, в которой ИБ между ретрансляторами (hop-by-hop), не была установлена доверительная связь. Например, Алис доверяет ее местному прокси-серверу. Этот прокси-сервер после обмена сертификатами доверяет местному прокси-серверу Боба, которому доверяет и Боб. Поэтому Боб и Алис взаимно аутентифицированы и могут безопасно общаться. TLS не является полностью независимым от приложения SIP. Необходимо, чтобы TLS в сетях SIP использовал как минимум (в соответствии с требованиями стандарта RFC 3261) протокол шифрования с открытым ключом RSA, протокол шифрования с общим ключом AES и длиной ключа 128 бит. Для совместимости требуется также поддержка протокола тройной DES. Могут использоваться и другие протоколы.

Схема с указанием в запросах и ответах sips, а не sip означает требование процедур обеспечения ИБ. Присутствие в поле заголовка Request-URI sips означает, что каждый ретрансляционный участок, через который посылается запрос, должен быть защищен с помощью протокола TLS. Как только запрос достигает локального домена вызываемого пользователя, вполне возможно он пересылается на последнем участке к серверу агента пользователя UAS с использованием протокола TLS. Должна быть подтверждена подлинность полученных в процессе аутентификации сертификатов с помощью корневых сертификатов, содержащихся у клиента. Отказ в подлинности сертификата служит основанием в отказе на запрос.

18.2.3.3. Механизм ИБ SIP-сети на базе протокола S/MIME

Протокол S/MIME (Secure/MIME, защищенный MIME) так же, как и TLS обеспечивает аутентификацию, целостность сообщений и шифрование. Для обеспечения этих функций в предыдущей версии стандарта по SIP (RFC 2543) был предусмотрен другой протокол безопасности электронной почты – PGP, описание которого приведено в главе 13.

С точки зрения общих функциональных возможностей обеспечения ИБ протоколы защиты электронной почты S/MIME и PGP очень похожи [9]. Оба протокола обеспечивают шифрование и цифровую подпись.

В сети SIP S/MIME обеспечивает шифрование сообщений сигнализации из конца в конец, а TLS обеспечивает шифрование/дешифрование между смежными узлами (hop-by-hop).

S/MIME – это дополнение протокола электронной почты MIME спецификацией безопасности. В S/MIME защита объекта MIME обеспечивается цифровой подписью, шифрованием или и тем и другим одновременно. Объектом MIME может быть как все сообщение, так и одна или несколько частей сообщения (multipart). Объект MIME вместе с

некоторыми связанными с ним данными защиты (например, сертификатами, идентификаторами алгоритмов шифрования и хеширования) обрабатываются средствами S/MIME, чтобы получить то, что обычно называется объектом PKCS и означает «спецификация криптографии с открытым ключом» (Public Key Cryptography Specificaton).

В S/MIME определены следующие типы содержимого:

- multipart/signed (открытое подписанное сообщение из двух частей – сообщение и его подпись). В сети SIP этот тип обеспечивает целостность и аутентификацию. Открытая часть сообщения является телом запроса SIP.

- application/pkcs7-mime (приложение). Это позволяет шифровать отдельно из конца в конец тело сообщения, не воздействуя на заголовок.

Этот тип содержит два блока – подтип шифрования объекта S/MIME или упакованных данных (envelopedData) и блок подписанные данные (signedData).

Блок envelopedData выполняет следующие действия:

- генерирует псевдослучайный сеансовый ключ;
- шифруется открытым ключом получателя сеансовый ключ (создается цифровой конверт);
- формируется *блок информации для получателя*, в который входят сертификат открытого ключа отправителя, цифровой конверт (зашифрованный открытым ключом отправителя сеансовый ключ), идентификатор алгоритма шифрования и сообщение;
- этот блок информации шифруется с помощью сеансового ключа.

Блоки информации для получателя, за которыми следует зашифрованное сообщение, вместе составляют блок envelopedData. Вся эта информация кодируется в формате Radix64 (см. глава 13, протокол PGP). Результат такой обработки называется объектом.

На приеме объекта сначала снимается кодировка, с помощью закрытого ключа получателя определяется сеансовый ключ, а затем расшифровывается принятое сообщение.

Блок signedData выполняет следующие действия:

- выбирается алгоритм создания профиля сообщения (SHA-1 или MD5);
- вычисляется профиль сообщения, которое должно быть подписано;
- формируется цифровая подпись с помощью закрытого ключа отправителя;
- формируется *блок информации подписавшей стороны*, включающий сертификат его открытого ключа, идентификатор алгоритма шифрования и цифровую подпись. Объект signedData состоит из нескольких блоков информации подписавшей стороны и самого подписываемого сообщения. Объект может также включать набор сертификатов открытых

ключей, достаточный для того, чтобы составить цепочку от центра сертификации высшего уровня доверия к объекту, подписавшему документ. Эта информация затем кодируется в формате Radix64.

Чтобы восстановить подписанное сообщение и проверить подпись, получатель сначала снимает кодировку Radix64, а затем расшифровывает профиль сообщения открытым ключом подписавшего сообщение. После этого получатель проверяет его совпадение с вычисленным профилем полученного сообщения.

18.2.3.4. Механизм аутентификации пользователя в SIP-сети на базе протокола HTTP Digest

Протокол HTTP используется в Интернете при обмене документами между веб-клиентами и серверами. В простейшем случае агент пользователя устанавливает прямое соединение с сервером, на котором расположен нужный пользователю ресурс [30]. Примером может служить интернет-сервер, на котором размещается нужная страница. В таком примере между клиентом и сервером создается TCP соединение. Затем клиент делает HTTP-запрос, который состоит из специфической команды, адреса URL (Uniform Resource Locator, унифицированный указатель информационного ресурса) и сообщения в формате MIME, содержащего параметры запроса, информацию о клиенте и другую информацию. Когда сервер получает запрос, он пытается выполнить его, а затем возвращает HTTP-ответ в формате MIME. Возможны между клиентом и сервером обработки запроса пользователя одна или более промежуточных систем, через которые транслируется запрос и ответ от сервера. В сетях HTTP в качестве промежуточных систем могут быть прокси-серверы, шлюзы, туннели и др.

Ответственность сервера SIP возложена на все три процедуры информационной безопасности – аутентификация, авторизация и учет, обычно обозначающим триединым термином AAA (Authentication, Authorization, Accounting). Все три процедуры связаны между собой. Например, учет использования ресурса для выставления счета имеет смысл, источник соединения подлинный, то есть аутентифицирован. После успешной аутентификации (authentication) следует определить на каких условиях (параметры качества обслуживания, виды услуг и др.) ему может быть предоставлен доступ. Эта процедура относится к авторизации (authorization). Выставление счетов за услуги основывается на длительности соединения и потребленных при этом ресурсах. Сбор такого рода информации осуществляется в рамках процедур учета (accounting). Все три функции AAA могут быть

вставлены в SIP сервер или быть во внешнем сервере. Если используется внешний сервер, то он выполняет функции протокола RADIUS. Название протокола складывается из первых букв слов – Remote Authentication Dial in User Service (услуга удаленной аутентификации вызывающего пользователя). Это определение не точно, так как описывает только одну (хотя и чаще всего применяемую) процедуру из AAA – аутентификацию пользователя для получения доступа к сети.

Для обеспечения аутентификации в сети SIP может быть положен в основу принцип аутентификации для протокола HTTP, стандартизированный в документе RFC 2617 [59].

Определение подлинности источника запроса (аутентификация) важно по следующим причинам: пользователи должны знать с кем они разговаривают; операторы услуг должны знать кто должен платить за разговор и кому они должны предоставить приоритет. Защита от спама ничего не стоит, если ненадежное обеспечение аутентификации.

Основной механизм, используемый для определения подлинности источника SIP запроса, является схема «Digest», которая базируется на принципах аутентификации для протокола HTTP (HTTP Digest Authentication). Она основана на общем пароле в сервере и у клиента. Этот протокол «вызов-ответ» использует хеш-код MD5 (128 бит) пароля пользователя, который по открытому каналу в адрес сервера передает измененный пароль. Сервер может проверить поступивший хешированный пароль, но перехвативший его злоумышленник не может по нему восстановить пароль. Хеш-функция формируется из пароля и дополнительных нескольких значений. Для того чтобы защититься от угрозы повтора перехваченного злоумышленником хеш-кода и повторно отправленного им в адрес сервера, хеш-код включает ранее полученное со стороны сервера случайное число (нонс). В результате хеш-код становится не постоянной величиной. Хеш-код включает также несколько значений самого SIP сообщения. Сервер проверяет полученный вызов. Для этого он рассчитывает собственный хеш-код, сравнивает его с принятым от клиента. Если они совпадают, то сервер убеждается в подлинности клиента. В качестве сервера при использовании такого механизма аутентификации может быть прокси-сервер или сервер регистрации.

Предусмотрено использование механизма аутентификации на базе схемы «Digest» в следующих процедурах:

- пользователь-пользователь. При этом производится аутентификация между UAC и UAS. UAS может быть, например, вызываемым пользователем или сервером регистрации SIP. В первом случае аутентификация имеет место при запросе вызова, во втором – во время регистрации;

- пользователь-прокси. При этом производится аутентификация между UAC и прокси-сервером SIP при запросе вызова.

Аутентификация пользователь-пользователь

Приведем последовательность шагов примера аутентификации пользователь-пользователь в случае сервера регистрации. Она включает обмен четырьмя сообщениями.

1. **Начальный запрос.** Агент UAC отправляет запрос в сервер (например, в сервер регистрации SIP) - INVITE sip:bob@biloxicom
2. **Вызов (challenge)**. Сервер регистрации отправляет ответ – 401 Unauthorized (с кодом 401, не авторизирован), сообщение которого содержит заголовок *WWW-Authentication*, в котором следующие параметры:

- Realm – содержит имя хоста или доменное имя сервера, исполняющего аутентификацию и используется для того, чтобы спрятать пароль и имя пользователя – WWW-Authenticate: Digest realm=" biloxi.com" .
- Показатель качества защиты (qop) – может быть "auth" , "auth int" или не указан. В зависимости от этого показателя определяются схемы расчета ответа серверу, которые приводятся ниже в настоящем разделе.
- Nonce (нонс сервера, т.е. случайное число) – сгенерировано сервером и используется клиентом для расчета ответа. Нонс сервера состоит из штампа времени, связанного с хеш-кодом, рассчитанным по штампу времени и паролю сервера. Эта схема обеспечивает защиту от повтора, исходя из свежести нонса, который возвратится в заголовке *Authorization* (авторизация) последующих запросов: nonce="dcd98b7102dd210e8b11ddf6ddbf0c093"
- Opaque – содержит данные, которые должны вернуться от агента UAC в заголовке *Authorization* (авторизация) последующего запроса. Сервер может использовать это поле для того, чтобы сохранить эту информацию, связанную с сеансом аутентификации: opaque= "5ccc069c4d3ebaf9fd17e95f4de41"
- Алгоритм – MD5 или MD5-sess. Эти алгоритмы отличаются между собой схемой расчета ответа агента UAC в адрес сервера.

3. Ответ (response). UAC рассчитывает ответ и передает серверу новый запрос. На этот раз заголовок этого запроса включает заголовок *Authorization авторизации*, который содержит следующие параметры.

- Имя пользователя – имя пользователя в realm: INVITE sip:bob@biloxicom, Authorization Digest username=”bob”
- Realm – то же, что в заголовке *WWW-Authentication* - realm=” biloxi.com”
- Nonce – то же, что в заголовке *WWW-Authentication*: nonce=”dcd98b7102dd210e8b11ddf6ddbf0c093”
- Digest URI (uri) – значение URI. Запрос URI может меняться при транзите: un= sip:bob@biloxicom
- Показатель качества защиты (qop) – указывает качество защиты, выбранное UAC: qop=auth,
- Счетчик нонса (nonce count, nc) – указывает на число различных запросов, отправленных UAC, использующих значение нонса в этом запросе. Счетчик нонса используется для защиты от угрозы повтора: n=00000001
- Если в заголовке имеется параметр показателя качества защиты gop, то в заголовке должен присутствовать параметр cnonce – нонс клиента: cnonce=”0a41113b”. Этот параметр (случайное число) генерирует клиент для расчета и проверки ответа. Это предусмотрено для защиты открытого пароля злоумышленником, представившимся сервером. Нонс клиента позволяет защищать от угрозы повтор за счет введения случайного характера в передаваемом сообщении.
- Ответ – рассчитанное агентом UAC значение **ответ**: response=”6629fae49393a05397450978507c4ef1”
- Opaque - то же, что в заголовке в сообщении 2 WWW-Authentication: opaque= “5ccc069c4d3ebaf9fd17e95f4de41”
- Алгоритм MD5 или MD5-sess - то же, что в заголовке WWW-Authentication.

Аутентификация пользователя считается успешной, если произведенный сервером расчет значения **ответ** по параметрам в заголовке *WWW-Authentication* совпадает с поступившим значением **ответ** от UAC.

Далее приводится описание, каким образом производится расчет значения **ответ**. Используются следующие понятия: KD(secret, data) = H(secret|| “||”||data), где H означает применение хеш-функции MD5 соответственно к входным параметрам и unq(param), которые обозначают значения параметров”param”, указанных в кавычках.

Когда качество защиты есть “auth” или “auth-int”, ответ рассчитывается следующим образом

ответ = KD (H(A1), unq(nonce) || “:”||unq(cnonce)|| “:”|| unq(gop)|| “:”|| H(A2)) (1.1)

В том случае, кода параметр gop отсутствует

ответ = KD (H(A1), unq(nonce) || “:”|| H(A2)) (1.2)

Когда используется алгоритм MD5 входящее в выражения 1.1 и 1.2 значение A1 рассчитывается по следующей формуле

A1= unq(username)|| “:”||unq(realm)||“:”||passwd. (1.3)

Здесь “passwd” означает пароль пользователя.

Когда используется алгоритм “MD5-sess”, значение A1 рассчитывается по следующей формуле

A1=H(unq(username)||“:”||unq(realm)||“:”||unq(passwd)||”:”|| (unq(nonce)|| “:”||unq(cnonce) (1.4)

Как видно из формул, *ответ* включает среди других параметров хеширование пароля. В тех случаях, когда используется отдельный север аутентификации, сервер SIP получает значение H(A1) из сервера аутентификации.

Когда качество защиты “auth” или не специфицировано, значение A2 определяется по формуле

A2=method||”:”||URI. (1.5)

Здесь “method” обозначает имя метода SIP. Если определено качество защиты “auth-int” специфицировано значение A2 определяется по формуле

A2=method||”:”||URI||”:”||H(bady). (1.6)

Здесь “bady” означает тело заголовка запроса SIP, целостность которого защищена с помощью хеширования.

4. Взаимная аутентификация. В том случае, если аутентификация пользователя завершилась успешно, выполняется процедура аутентификации сервера регистрации. При этом сервер отправляет ответ с кодом 200 (ОК), в сообщении которого содержится заголовок *Authentication-Info*, включающий следующие параметры.

- Nextnonce – генерирует еще один нонс (случайное число), которое UAC должен будет использовать для аутентификации сервера при следующем запросе;
- Показатель качества защиты (qop) – указывается качества защиты, которое обеспечивает сервером к сообщению *ответа*.
- Нонс клиента (cnonce) – то же, что обеспечивается клиентом сообщении 3 в заголовке авторизации Authrithation.
- Счетчик нонса (nonce count, nc) – копия счетчика нонса сервера в сообщении 3.
- Response authentication (rspauth) – рассчитанный сервером **ответ** для того, чтобы доказать, что он знает пароль пользователя. Для **ответа** сервера используются те же равенства, что и для **ответа** клиента (выражения 1.1 и 1.2). Исключение составляет определение A2.

Когда качество защиты принято “auth” или не специфицировано, A2 рассчитывается для ответа при аутентификации сервера по формуле

A2=”:”||URI.

Если качество защиты “auth-int”, то

A2=”:”||URI ||”:”||H(bady).

Здесь “bady” означает тело заголовка ответа SIP, целостность которого защищена с помощью хеширования.

Аутентификация сервера считается успешной, если произведенный UAC расчет значения **ответ** по параметрам в заголовке *Authentication-Info* совпадает с поступившим значение **ответ** от сервера.

Аутентификация пользователь-прокси

Семантика заголовков *Proxy-Authentication, Proxy-Authorization, Proxy-Authentication-Info* подобна заголовкам *WWW-Authentication, Authentication, Authentication-Info.*

Процедура аутентификации состоит из следующих шагов.

Если запрос SIP не содержит заголовок *Proxy-Authentication*, то сервер отправляет ответ 407 (Аутентификация прокси-сервера обязательна). Приняв ответ 407, UAC использует параметры **вызова (challenge)** из этого заголовка и производит расчет **ответа** (response) аналогично тому, как это делается при аутентификации пользователь-пользователь и показано выше. Значение этого **ответа** включено в заголовок следующего запроса INVITE.

Прокси-сервер проверяет ответ UAC и может завершить аутентификацию пользователя. Прокси-сервер может также аутентифицировать себя пользователем UAC. При этом сервер отправляет ответ с кодом 200 (ОК), в сообщении которого содержится заголовок *Proxy-Authentication-Info*, включающий необходимые параметры. Эта процедура аналогична этапу взаимной аутентификации пользователь-пользователь.

Если следующий нонс установлен в заголовке *Proxy-Authentication-Info,* UAC сохраняет это значение, а также добавляет единицу в счетчик нонса (nonce count, nc) для того, проводить аутентификацию при следующих запросах.

18.2.3.5. Аутентификация идентификатора пользователя

В работе [54] приводятся данные ассоциации по контролю за мошенничеством CFCA (Communication Fraud Control Association), направленным на использование услуг связи без их оплаты, т.е. за фродом. Согласно этим данным в результате фрода ежегодные потери для операторов традиционных сетей связи составляют 3-5% от доходов оператора и величина таких потерь ежегодно увеличивается на 10%. По результатам анализа этой организации следует, что угрозы фрода и потери операторов в сетях VoIP выше.

Схема HTTP Digest Authentication остается наиболее используемым механизмом аутентификации в SIP, но ей свойственны некоторые слабости в защите от угроз. Многие исследования в этом отношении связывают с протоколом хеширования MD5. Другая проблема слабости этой схемы как отмечено в документе RFC 4474, связана с необходимостью организации установления паролей у аутентификатора и пользователя. Для создания хеш-кода MD5 необходим ввод открытого текста пароля. В базе данных хранятся хеш-коды MD5 пароля, имя пользователя (username) и доменное имя (realm). Для того чтобы риски безопасности были удовлетворительными, необходимо эти данные хорошо защитить.

Даже при успешном решении всех этих задач остается проблема защиты от фальсификации и других манипуляций с идентификатором *From*, расположенным в поле заголовка запроса SIP.

В идентификаторе содержится адрес URI отправителя запроса. При этом рассматриваются следующие угрозы ИБ и последствия при их реализации:

- кража идентификатора другим пользователем-нарушителем, который начинает пользоваться всеми услугами легитимного пользователя. В результате он получает доступ к определенным услугам;
- кража подписки. В результате такой кражи идентификатора, при которой нарушитель получает вызовы, предназначенные для легитимных пользователей;
- приватность. Вызываемый пользователь хотел бы иметь некоторую гарантию того, что вызывающий пользователь тот, за которого себя выдает. Вызывающий пользователь часто желает спрятать свой идентификатор от вызываемого пользователя и не доверенного провайдера услуг. Для того чтобы обеспечить приватность вызывающего пользователя информация его идентификатора должна быть скрыта таким же образом, как зашифровывается информация от не доверенных провайдеров услуг. При этом необходимо также обеспечить возможность маршрутизации. Кроме этого требуется обеспечить возможность предоставления счетов за предоставленные пользователям услуги связи. Поэтому должен быть использован механизм обеспечения ИБ из конца в конец.

Протокол RFC 3261 не определяет механизм защиты от угроз идентификатору. Самым надежным решением является использование пользователями аутентификации с помощью сертификатов, что представляет практические трудности реализации. Поэтому протокол RFC 4474 [60] предлагает в качестве промежуточного более простой вариант, основанный на концепции «сервис аутентификации» и введении нового заголовка SIP – Идентификатор. Для того чтобы пояснить принятый RFC алгоритм аутентификации идентификатора RFC 4474 приведем пример реализации: Алис желает установить сеанс с Бобом. sip:Alice@example.com; sip:Bob@example.org.

Алис отправляет запрос INVITE с полем заголовка *From*, который используя протокол TLS поступает на прокси-сервер, выполняющий функцию сервиса аутентификации ее домена. Сервис аутентификации аутентифицирует Алис (возможно отправляя вызов HTTP Digest Authentication) и подтверждает подлинность идентификатора в поле заголовка *From*. Прокси-сервер, выполняющий функцию сервиса аутентификации, определяет хеш-функцию данных, включающих поле заголовка *From* и тело заголовка, подписывает закрытым ключом сертификата домена (в данном случае домена example.com) и вставляет его в новое поле заголовка - Идентификатор. Прокси-сервер, выполняющий функцию сервиса аутентификации домена, в котором расположен Боб, расшифровывает эту подпись и

убеждается в аутентификации источника, в подлинности идентификатора в поле заголовка *From*. Та же самая проверка подлинности может быть выполнена сервером агента пользователя UAS.

18.3. Транспортировка данных в сети SIP

18.3.1. Протоколы транспортировки данных

Полезная нагрузка в IP-пакете каждого мультимедийного приложения VoIP переносится с помощью транспортного протокола реального масштаба времени RTP. В стандарте RFC 1889, где описан этот протокол, не предусмотрены механизмы контроля ошибок и повтора передачи. Этот протокол работает поверх протокола UDP, что обеспечивает выполнение этих функций и малую величину задержки для речевых сигналов. Напомним, что величина задержки является одним из основных показателей качества обслуживания QoS при передаче речи по сети связи. Одним из источников задержки является обработка речевого кадра в кодеке. Кодек осуществляет сжатие голосовых данных, что позволяет эффективно использовать пропускную способность IP-канала. В таблице 18.2. приведены характеристики кодеков четырех стандартов ITU-T: G.723, G.729, G.729A, G.728. Здесь указаны следующие показатели.

Таблица 18.2. Характеристики кодеков

Кодек	Скорость передачи, кбит/с	Задержка	MOS
G.723	5,3; 6,3	Высокая (37 мс)	3,7; 3,8
G.729	8	Низкая (10 мс)	4
G.729a	8	Низкая (10 мс)	3,4
G.728	16	Очень низкая (3-5 мс)	4,1

- Скорость передачи речи после сжатия основного цифрового канала 64 кбит/с.
- Задержка.
- Усредненная оценка разборчивости речи MOS (Mean Opinion Score). Этот показатель является субъективным эталоном для проверки эффективности голосового кодека. Разборчивость речи MOS оценивается в пределах от 1 (плохо) до 5 (превосходно).

Стандарт G.729 с алгоритмом кодирования (CS-ACELP, Conjugate StructurAlgebraic Code Excited Lineaar Predictive, algorithm) *алгоритм линейного предсказания (по кодовой книге) с возбуждением сопряженным структурированным алгебраическим кодом* получил широкое распространение в VoIP. Этот протокол в стеке протоколов модели TCP/IP принадлежит прикладному уровню. В то же время он является общим, независимым протоколом для разных мультимедийных приложений (VoIP, музыка и видео по заказу, видеоконференции и др.). Поэтому в работе [10] протокол RTP определен транспортным протоколом, реализованным на прикладном уровне. Заголовок RTP состоит из трех 4-х байтовых слов и некоторых возможных расширений. Приведем содержание некоторых полей:

Счетчик 16 бит, который инкрементируется каждым обработанным пакетом. Предназначен для определения потерянных пакетов. Поле *тип данных*, который указывает тип кодека. Поле *отметки времени*, которое отмечает момент создания первого слова пакета, и предназначено для снижения характеристики джиттера.

Один пакет RTP, кодированный по стандарту G.729, включает созданную в сжатом виде полезную нагрузку длиной 10 байтов (при передаче 10 мс ревой информации). К ней добавляются заголовки RTP (12 байтов), заголовок UDP (8 байтов), IP-заголовок (20 байтов). При таком большом поле заголовков падает эффективность использовании полосы пропускания при реализации сжатия. Поэтому в VoIP обычно используется передача

нескольких кадров в пакете. Часто в одном пакете передается до 120 мс речевой информации. В заголовок RTP входит поле, определяющее число CSRC-полей в конце заголовка, т.е. число источников, формирующих поток. В заголовок входит также поле источника синхронизации SSRC, которое идентифицирует этот источник.

Все перечисленные поля составляют фиксированную часть заголовка, за которым следуют еще 15 отдельных 32-разрядных CSRC полей, которые идентифицируют источники данных.

Для передачи информации о потоке RTP используется протокол управления в реальном масштабе времени RTCP (Real Time Transport Control Protocol). Этот протокол обеспечивает информацией о показателях качества обслуживания QoS, обеспечиваемых протоколом RTP, - время задержки, джиттер, доля потерянных пакетов. Эта информация дает возможность, например, уменьшить коэффициент сжатия информации (сменой кодека) с целью улучшения качества ее передачи.

18.3.2. Обеспечение ИБ при транспортировке данных

Для обеспечения шифрования и аутентификации транспортируемых данных в сетях VoIP были разработан стандарт RFC 3711, включающий протокол безопасности SRTP (Secure RTP) для протокола RTP и протокол безопасности SRTSP (Secure RTSP) для протокола RTSP. В заголовок SRTP рекомендуется использовать поле для метки аутентификации и опционно поле идентификатора мастер-ключа MKI (Master key Identifier). Ниже приводится описание функции MKI. Поле заголовка SRTP не шифруется. Заголовок SRTSP также не шифруется. Аутентификации подлежит весь заголовок SRTP, кроме кода аутентификации и поля MKI. Аутентификация основной части заголовка и полезной нагрузки RTCP осуществляется с помощью механизма MAC (см. приложение Г). Некоторые технологии беспроводного доступа позволяют значительные потери эффективности при увеличении длины дейтаграмм RTP, а другие технологии вовсе не допускают никакого увеличения дейтаграмм. В последнем случае длина поля аутентификации меньше, чем 80 бит. Реальный масштаб времени накладывает на RTP следующие требования по передаче и обработке транспортируемых данных.

- Шифрование и дешифрование должно быть обеспечено, несмотря на потери или нарушение порядка поступления дейтаграмм.
- Процесс дешифрования должен начинаться до поступления на прием всех данных.

Кроме поля полезной нагрузки в состав пакета безопасности SRTP входит заголовок со следующими параметрами.

- *Счетчик* 48 бит, который инкрементируется каждым обработанным пакетом.
- *Номер последнего пакета*, принятого на обработку.
- *Список номеров пакетов* для защиты от атаки повтора (при обеспечении аутентификации и защиты от повтора).

Шифрование полезной нагрузки

В соответствии со стандартом RFC 3711 возможно использовать протокол шифровании с общим ключом AES. Предложен алгоритм аутентификации сообщений HMAC с использованием хеш-кода SHA1. Один мастер-ключ должен быть использован для защиты максимально 2^{48} RTP дейтаграмм или 2^{32} RTCP дейтаграмм. После этого мастер-ключ должен быть сменен. Предоставлена возможность и более частая смена мастер ключа.

Мастер-ключ используется для создания сеансовых ключей. Сеансовый ключ используется для шифрования данных и для аутентификации сообщений. Для этого требуется шесть различных сеансовых ключей: два ключа шифрования данных SRTP/SRTCP, два ключа для шифрования вектора инициализации IV с целью повышения стойкости механизма защиты ключей шифрования данных SRTP/SRTCP и два ключа аутентификации для SRTP/SRTCP. Поэтому протоколу управления ключами необходимо обменяться только одним мастер-ключом с ключом шифрования вектора инициализации, а затем местный SRTP генерирует все ключи сеансов.

ГЛАВА 19. Управление сетью сигнализации ОКС№7

19.1. Управление сетью сигнализации

Под функцией управления сетью сигнализации принимаются алгоритмы и протоколы их реализации в процессе эксплуатации по поддержанию работоспособности ОКС №7 и восстановлению ЗС и пунктов сигнализации при отказах, перегрузках и др. Изменение состояния ЗС и пунктов сигнализации могут вызвать необходимость коррекции таблицы маршрутизации. На рис. 17.8 (глава 17) приведен формат сообщения MSU, выполняющего функцию MTP по управлению сетью сигнализации. Переход к службе управления сетью сигнализации устанавливается в поле индикатора вида службы SI. В поле сигнальной информации SIF содержатся сообщения управления сетью сигнализации, включающие идентификатор сообщения (группа сообщений и тип сообщения этой группы сообщений) и информацию, относящуюся к выполнению определенной функции. Реализация функций управления сетью сигнализации осуществляется в результате обмена между пунктами сигнализации этими сообщениями управления сетью. Поле выбора звена сигнализации используется не для разделения нагрузки в сообщении ISUP между ЗС, а для выполнения команд по управлению сетью (например, перевод трафика на резервное звено ЗС). Поэтому здесь это поле называется SLC (Signaling Link Code- код звена сигнализации), а не SLS при выполнении функции разделения нагрузки.

Функции управления сетью сигнализации подразделяются на управление сигнальным трафиком, управление звеньями сигнализации и управление маршрутами сигнализации. Эти функции используются каждый раз, когда в сети происходит какое-нибудь событие (например, отказ или восстановление ЗС). Прежде, чем перейти к анализу каждой из этих функций приведем краткое описание некоторых из основных состояний ЗС, маршрута сигнализации и пункта сигнализации.

Каждое ЗС рассматривается уровнем MTP3 как доступное или недоступное для переноса сигнального трафика. В частности, ЗС становится недоступным, если оно находится в состоянии:

- отказа (при высокой интенсивности ошибок, превышении отведенного времени для начального фазирования, превышении допустимого времени перегрузки и др.);
- деактивации, т.е. удалении из работы (при получении указания от системы

эксплуатационного управления и др.);

- заблокировано (при обнаружении отказа собственного процессора уровня МТР3 или такого же процессора на удаленном конце ЗС и др.).

Сигнальный маршрут рассматривается уровнем МТР3 как доступный, ограниченно доступный или недоступный. Переход в каждое из этих состояний происходит при получении определенных сообщений MSU в режиме управления сетью.

Пункт сигнализации может быть недоступным и доступным. Различают недоступность собственно пункта сигнализации и недосягаемость смежного пункта сигнализации. Пункт сигнализации становится недоступным, когда все подсоединенные к нему ЗС недоступны. Смежный пункт сигнализации рассматривается как недосягаемый, если все звенья, ведущие к нему напрямую недоступны. Любое изменение статуса ЗС, сигнальных маршрутов или пунктов сигнализации требует применения указанных выше функций управления сетью сигнализации-управления сигнальным трафиком, управления ЗС и управления сигнальным маршрутом.

19.1.1. Управление сигнальным трафиком

Процедуры управления сигнальным трафиком применяются (в случаях неисправности устройств сети или перегрузок) при необходимости перевода трафика из нормального звена (звеньев) и маршрута (маршрутов) на одно или несколько резервных звеньев или маршрутов, для перезапуска пункта сигнализации или для временного ограничения интенсивности сигнального трафика в случае перегрузки в пункте сигнализации. Рассмотрим некоторые из этих процедур.

19.1.1.1. Процедуры перевода трафика на резервное ЗС и возврата на исходное ЗС

На рис. 19.1 показан перевод трафика на резервное ЗС. Возможно два случая перевода – в одном пучке ЗС (рис. 19.1, а) и в разных ЗС, находящихся в разных маршрутах (рис. 19.1, б)

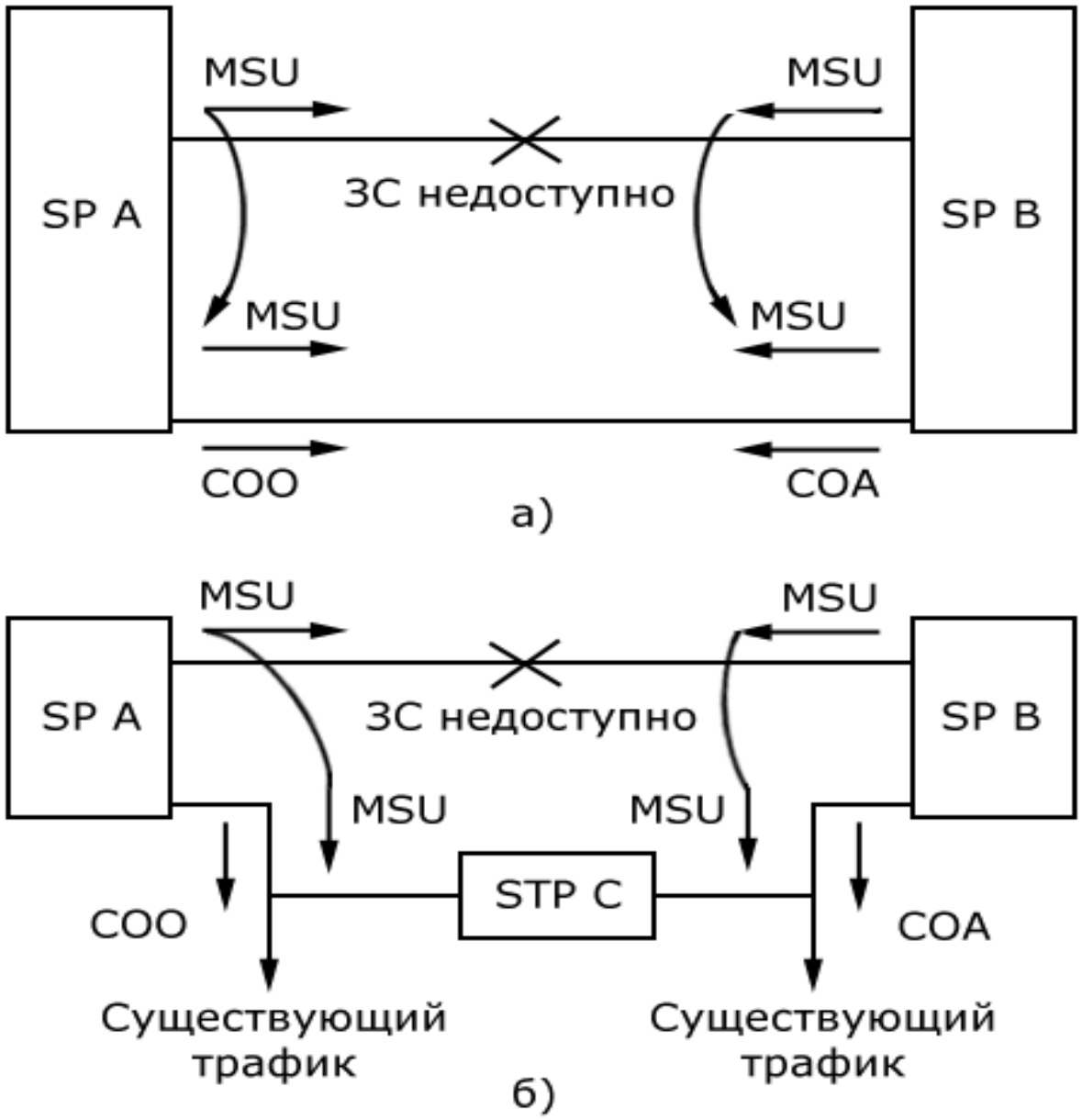


Рис. 19.1. Перевод трафика на резервное ЗС

Инициирующий перевод трафика на резервное ЗС SP передает в сторону противоположного SP команду сигнализации COO (Changeover order) о переводе трафика на резервное звено. В ответ он должен получить команду подтверждения перевода трафика COA (Changeover Acknowledgement). Эти команды (сообщения) относятся к режиму управления сетью и содержат в поле SI заголовка (рис. 17.8, глава 17) соответствующее значение (0000). Всё поле SIF, кроме этикетки сообщений управления сетью используется для размещения команд управления сетью сигнализации. Каждая команда управления, кроме идентификатора типа, включает в своих форматах другие параметры.

Формат команд COO и COA включает номер последней успешно принятой MSU противоположной стороны ЗС. Это позволяет предотвратить потери, дублирования или нарушения очередности передачи сообщений. Процедура перевода трафика на резервное звено использует этот параметр для считывания сообщения из буферной памяти недоступного ЗС в буферную память резервного ЗС. Эти считанные сообщения являются неподтвержденными удаленной стороной и подлежат передаче по резервному ЗС. Значение в поле кода звена сигнализации (SLC) идентифицирует недоступное ЗС.

В некоторых случаях (например, из-за отказа сигнального терминала) может возникнуть ситуация, в которой на соответствующей стороне недоступного звена невозможно будет определить номер последней MSU, успешно принятой по недоступному каналу. В этом случае используется процедура аварийного перевода трафика на резервное ЗС. При этом используются команды ECO (Emergency Changeover Order) и ECA (Emergency Changeover Acknowledgement).

В формате этих сообщений в отличие от сообщений COA и COO отсутствует поле номера последней успешно принятой MSU.

Процедура возврата трафика на исходное звено применяется для перевода сигнального трафика с резервного ЗС на ставшее вновь доступным исходное ЗС. Ранее недоступное ЗС становится вновь доступным, т.е. после восстановления, разблокирования или отмены запрета доступа. По резервному ЗС на удаленный пункт сигнализации передается команда CBD (Changeback Declaration) о возврате на исходное ЗС, указывающее на то, что никаких сообщений потока трафика, подлежащего возврату по этому звену, больше передавать не будет. Пункт сигнализации возобновляет перенос трафика по ставшему вновь доступным ЗС после получения команды CBA (Changeback Acknowlegement) подтверждения возврата на исходное ЗС от удаленного пункта сигнализации. Сообщение подтверждения указывает, что сигнальные сообщения соответствующего потока, направляемые на удаленный пункт сигнализации по резервному ЗС, были приняты. Приняв команду CBA, пункт сигнализации возобновляет перенос трафика по вновь ставшему доступным ЗС. Время ожидания ответного сообщения CBA ограничено таймером T4 = 0,5 – 1,2 сек; если за время T4 сообщение CBA не поступает, то сообщение CBD повторяется. При повторной попытке запускается таймер T5 = 0,5 – 1,2 сек. Если ответное сообщение CBA опять не поступает, то трафик возобновляется, но при этом извещается система техобслуживания. Команды CBD и CBA представляют собой также сообщения эксплуатационного управления сетью сигнализации.

19.1.1.2. Процедура вынужденной ремаршрутизации и управляемой ремаршрутизации

Целью процедуры вынужденного изменения маршрутизации (ремаршрутизации) является восстановление способности переноса сигнальных сообщений между двумя смежными пунктами в направлении к определенному пункту назначения. Процедура управляемой маршрутизации применяется, когда сигнальный маршрут в направлении определенного пункта назначения вновь оказывается доступным (например, после устранения отказов в удаленных элементах сети сигнализации), и становится возможной процедура обратного перевода трафика с резервного на нормальный сигнальный маршрут. Пример указанных процедур приведен на рис. 19.2.

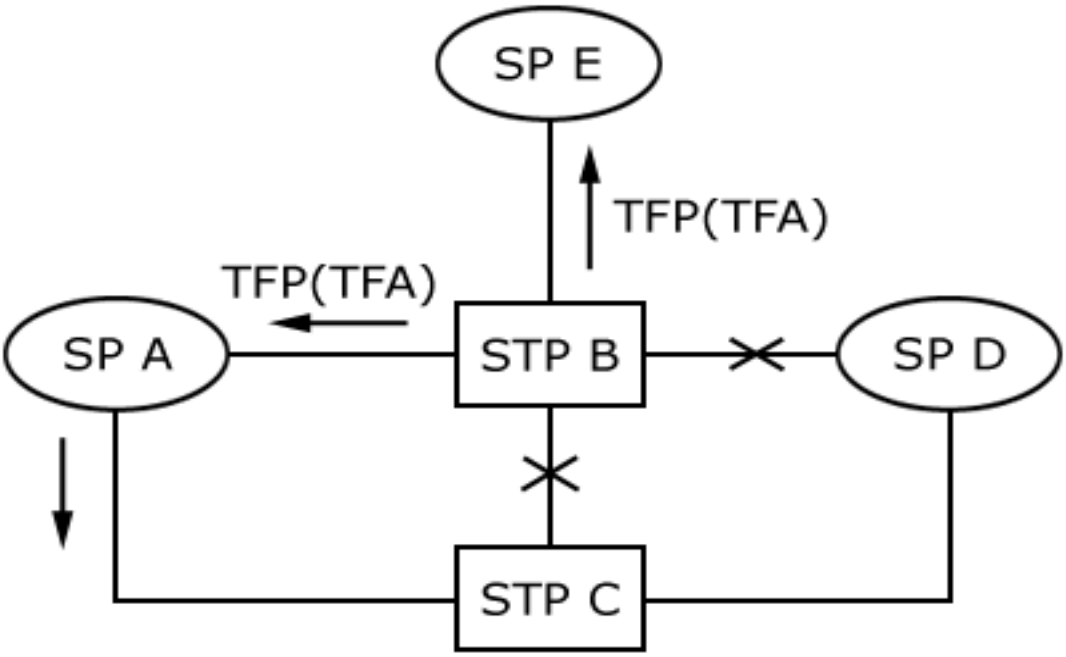


Рис. 19.2. Процедура вынужденной ремаршрутизации и управляемой ремаршрутизации

Процедура вынужденной ремаршрутизации инициируется в пункте SP A при приеме сообщения TFP (Transfer Prohibited) о запрещении переноса со стороны смежного транзитного пункта сигнализации STP B. Это сообщение указывает на невозможность доставки MSU к пункту назначения SP D из-за отказа звеньев сигнализации SP D-STP B и SP D-STP C.

В пункте сигнализации, получившем сообщение TFP, выполняется следующая последовательность действий:

- останавливается перенос сигнального трафика по недоступному сигнальному

маршруту (SP A-STP B-SP D), после чего в буфере ЗС сохраняется часть не переданного трафика;

- определяется резервный сигнальный маршрут (SP A-STP C-SP D);
- перенос сигнального трафика восстанавливается, начиная с содержимого буфера ЗС, по пучку ЗС, относящемуся к резервному сигнальному маршруту. Формат сообщения TFP включает поле адреса пункта назначения, к которому относится это сообщение (в данном случае адрес SP D).

Процедура управляемой ремаршрутизации (восстановление маршрута) инициируется в пункте сигнализации при приеме сообщения TFA (Transfer Allowed), которое указывает на восстановление возможности доставки сообщения к пункту назначения (SP D). Эта ситуация возникает при восстановлении ЗС между STP B и SP D. Формат сообщений TFA (указанных на рис. 19.2 в скобках) отличается от TFP только значением в поле типа сообщения.

19.1.1.3. Процедура перезапуска MTP

Пункт сигнализации недоступен, когда все подсоединенные к нему ЗС недоступны. За время такой изоляции состояния смежных и удаленных пунктов сигнализации, а также пучков ЗС могли измениться. Восстановление такого пункта сигнализации требует процедуры выдержки времени, в течение которой необходимо уточнить состояние ЗС и пунктов сигнализации в таблице маршрутизации. Такая процедура перезапуска MTP предусматривает ее завершение, если активизировано достаточное количество ЗС, при котором не возникает повторного отказа этого пункта сигнализации. В случае кратковременной изоляции пункта сигнализации (менее 500-1200 мсек) процедура перезапуска не производится.

Во время перезапуска производится обмен сообщениями управления сетью между пунктом перезапуска и смежными пунктами. Определено максимальное время, в течение которого перезапуск должен быть успешно завершен. Приведем структуру сети и состояния ЗС перед первым этапом перезапуска STP D (рис. 19.3, а).

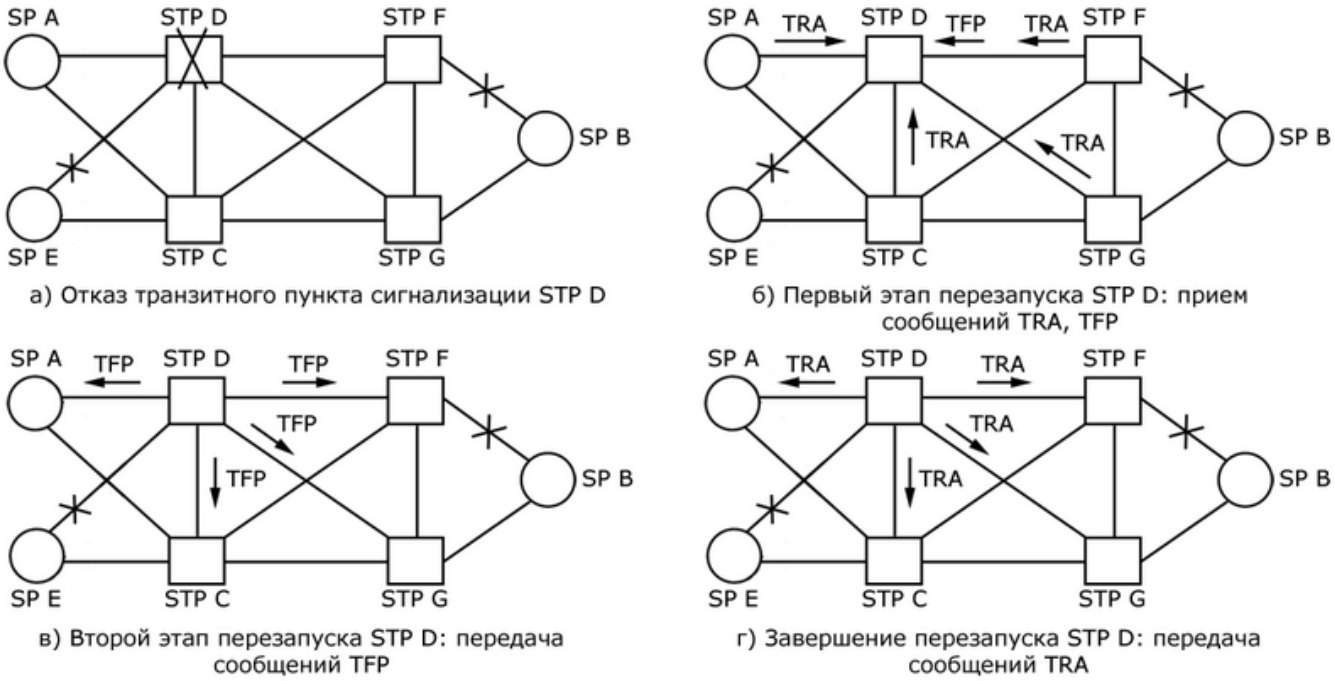


Рис. 19.3. Процедура перезапуска MTP

На первом этапе смежные с STP D пункты сигнализации используют сообщения TFP о состоянии их пунктов взаимодействия (рис. 19.3, б). Пункт SP F сообщает в TFP недоступность SP B. Остальные смежные пункты сообщений TFP не направляют. Формат TFP описан выше. Первый этап завершается приемом пункта перезапуска сообщения TRA (Traffic Restart Allowed) о разрешении перезапуска трафика. Эти сообщения поступают по всем активизированным ЗС. Формат TRA включает только поле типа сообщения. Сообщение TRA указывает, что вся информация о недоступных направлениях передана. Как видно из рис. 19.3, б), если направление доступно, то сообщение TRA передается без предварительной передачи TFP. По таким сообщениям TRA система управления перезапуском пункта сигнализации оценивает степень завершенности процесса уточнения состояния данных таблицы маршрутизации. После завершения первого этапа или по истечении выдержки времени T20=59-61сек, отведенной для процедуры, пункт перезапуска STP D передает всем смежным пунктам, доступным по прямым ЗС, сообщения TRA. Это указывает на завершение второго этапа (рис. 19.3, в). Во время второй фазы пункт перезапуска информирует смежные пункты о ЗС, которые в состоянии недоступности (TFP сообщает о недоступности пункта SPE).

Третий этап (рис. 19.3, г) завершает перезапуск STP D передачей сообщения TRA всем смежным пунктам по доступным ЗС. Запускается таймер (67-69 сек) для каждого

переданного сообщения TRA и возобновляется нормальная работа подсистемы MTP.

19.1.1.4. Процедура управляемого переноса

Процедура управляемого переноса в межународной сети используется с целью доставки с помощью сообщения TFC (Transfer Control) индикации перегрузки от пункта сигнализации, где обнаружена перегрузка, к исходящему пункту сигнализации. В формат сообщения TFC кроме типа сообщения входит поле, содержащее адрес пункта назначения, к которому относится сообщение.

В приведённом примере процедуры управляемого переноса (рис. 19.4) таким пунктом является STP F.

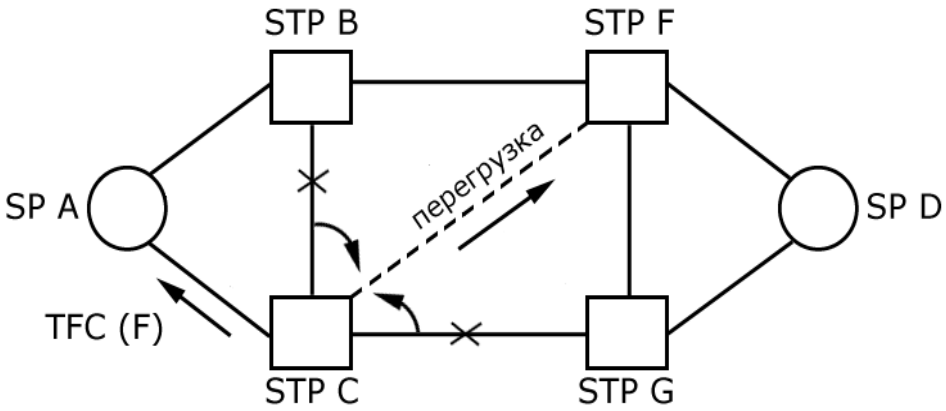


Рис. 19.4. Пример процедуры управляемого переноса

19.1.1.5. Недоступность подсистемы ISUP

Если MTP3 получает MSU, где в поле индикатора вида службы SI обнаруживается, что указанному там значению не соответствует ни одно из принятых подсистем, он не может доставить это сообщение никуда. В этом случае исходящему SP передается сообщение управления MTP3 «недоступность подсистемы ISUP» - UPU (Use Part Unavailable). В формат сообщения UPU входят два поля - идентификатор подсистемы пользователя и причина недоступности. Например, если пункт SP A отправляет сообщение ISUP к пункту SP B, в котором подсистема ISUP недоступная или отсутствует, MTP3 в пункте SP B передает SP A сообщение UPU со значением поля «идентификатор подсистемы пользователя», равным ISUP(0101). В поле «причина недоступности» указывается, почему эта подсистема недоступна.

19.1.2. Управление звеньями сигнализации

Управление звеньями сигнализации включает:

- активацию звена сигнализации;
- восстановление звена сигнализации;
- деактивацию звена сигнализации;
- активацию пучка звеньев сигнализации;
- назначение звена передачи данных (т.е. канала без сигнального терминала). Все перечисленные функции, кроме последней, выполняются с помощью обмена сообщениями второго уровня (MTP2), т.е. сигнальными единицами состояния звена (LSSU).

Процедура назначения звена передачи данных осуществляется с помощью сообщений управления сетью сигнализации на уровне MTP3. Автоматическое назначение звеньев передачи данных в качестве звена сигнализации может применяться при выполнении процедур выключения сигнального звена. Для замены такого ЗС может быть выбрано любое звено передачи данных, которое входит в группу разговорных каналов между пунктами сигнализации.

После того, как канал передачи первичного тракта выбран пунктом сигнализации для использования в качестве звена сигнализации в сторону удаленного пункта передается сообщение DLC (Signaling Data Link Connection Order) подключить назначенное звено передачи данных к сигнальному терминалу. В формате сообщения DLC содержится поле идентификатора звена передачи данных. В ответ на сообщение DLC встречный пункт передает одно из трех сообщений - результат попытки подключить звено передачи данных:

- подключение произведено CSS (Connection-Successful);
- подключение не произведено CNS (Connection-not-successful);
- подключение невозможно CNP (Connection-not-possible).

19.1.3. Управление сигнальными маршрутами

Функция управления сигнальными маршрутами используется для обеспечения надежного обмена между пунктами сигнализации информацией о недоступности сигнальных маршрутов. Информация недоступности, ограниченной или полной доступности сигнальных маршрутов передается в рамках процедур запрещения, ограничения и разрешения переноса сообщений. Некоторые элементы управления маршрутизацией были рассмотрены в

предыдущих подразделах управления сетью сигнализации при управлении сигнальным трафиком.

Кроме этих процедур в управление сигнальными маршрутами входит также процедура проверки (тестирования) пучка сигнальных маршрутов. Эта процедура позволяет SP определить возможность переноса сигнального трафика к определённому SP через смежный STP. На рис. 19.5 приведен пример выполнения процедуры проверки пучка сигнальных маршрутов. Процедура использует сообщение тестирования пучка маршрутов для пункта назначения, перенос к которому запрещён RST (Signalling-route-set-test-signal for prohibited destination) и сообщения TFP и TFA, описанные ранее при выполнении процедур вынужденной и управляемой ремаршрутизации. Процедура проверки пучка сигнальных маршрутов применяется для восстановлении информации о досягаемости направлений, которая потенциально могла быть утеряна вследствие отказов в сети сигнализации (на рис. 5. отказ ЗС STP D – SP B и STP D – STP C). Сообщение RST передается исходящим SP (в STP D) после приема TFP относительно SP назначения стороны смежного STP (SP B в примере).

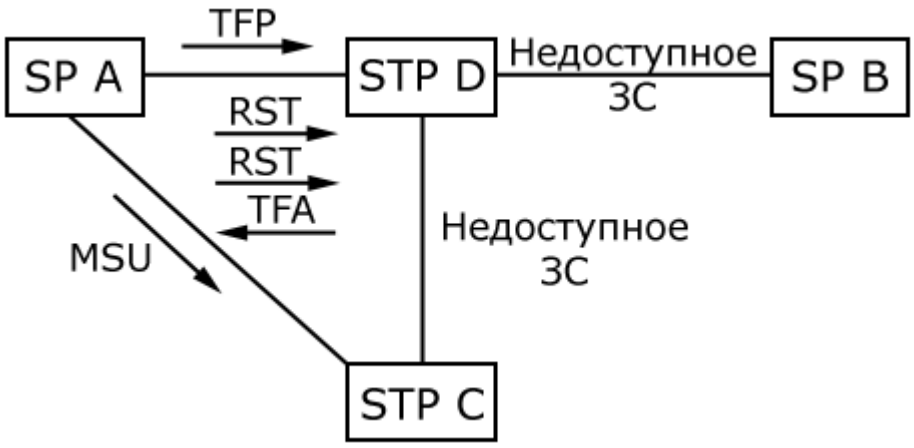


Рис. 19.5. Пример выполнения процедуры проверки пучка сигнальных маршрутов

Сообщения RST передаются с периодичностью (30-60 сек) до приема сообщений TFA из STP D, указывающего на то, что пункт назначения (SP B) вновь стал досягаем.

В формат сообщения RST входит поле, содержащее адрес пункта назначения, к которому относится это сообщение (в примере адрес SP B).

19.2. Тестирование звена сигнализации

После успешного выполнения процедур включения или восстановления звено сигнализации переходит в состояние обслуживания сигнального трафика. Однако доступным для переноса сигнального трафика подсистем-пользователей ЗС становится только после успешного проведения тестирования. Процедура тестирования сигнального звена приведена в рекомендации ITU-T Q.707. Тест сигнального звена проводится независимо с обеих его сторон и заключается в передаче через регулярные промежутки времени T2 (30-90сек) специальных сообщений.

Пункт сигнализации, инициировавший процедуру тестирования, передает встречному пункту сообщение тестирования звена сигнализации (SLTM, Signaling link test message). Это сообщение содержит тестовую информацию (произвольную последовательность битов), которая выбирается по усмотрению инициирующей стороны, и идентификатор звена в поле SLC. Получив сообщение SLTM, смежный пункт сигнализации передает по этому же звену сообщение подтверждения (SLTA, Signaling link test acknowledgement message), содержащее ту же тестовую информацию, которая была в сообщении SLTM.

Процедура тестирования звена считается успешно проведенной, если принятое сообщение подтверждения SLTA удовлетворяет следующим критериям:

- идентификатор звена SLC соответствует сигнальному звену, по которому было принято сообщение SLTA;
- код исходящего пункта сигнализации OPC определяет пункт сигнализации на дальнем конце звена;
- тестовая информация, содержащаяся в сообщении SLTA, аналогична переданной в SLTM.

Если же сообщение SLTA не удовлетворяет вышеуказанным критериям или, если ответное сообщение вообще не было получено в течение времени T1(4-12с), тест рассматривается как неуспешный и повторяется еще раз. В случае повторения отрицательного результата, звено выводится из обслуживания, и производится попытка его восстановления; при этом должна быть оповещена система эксплуатационного управления.

Сообщения группы тестирования и технического обслуживания сети сигнализации переносятся по звену, подлежащему тестированию, в значащих сигнальных единицах. Эти сообщения отличаются от других индикатором подсистемы (SI).

Этикетка сообщений тестирования и технического обслуживания сети сигнализации имеет ту же структуру, что и этикетка сообщений управления сетью сигнализации. Код заголовка

данной группы сообщений H0=0001.

Сообщения тестирования SLTM и подтверждения тестирования SLTA сигнального звена входят в группу тестирования звена сигнализации с индикатором вида службы SI=0001 (см. рис. 17.8, глава 17).

19.3. Пример отказа и восстановления сигнального звена сигнализации между исходящим и транзитным пунктами сигнализации

В разделах 19.1 и 19.2 настоящей главы показано функционирование некоторых отдельных функций по управлению сетью сигнализации. В настоящем и следующем разделах приводится описание использования этих функций при отказе и восстановлении:

- звена сигнализации между исходящим и транзитивным пунктами;
- транзитного пункта сигнализации.

Приведем алгоритм обмена сообщениями управления сетью сигнализации при отказе сигнального звена между исходящем и транзитным пунктами сигнализации, а также алгоритм при восстановлении работоспособности звена сигнализации. Рассмотрению подлежит участок сети ОКС№7, приведенный на рис. 19.6.

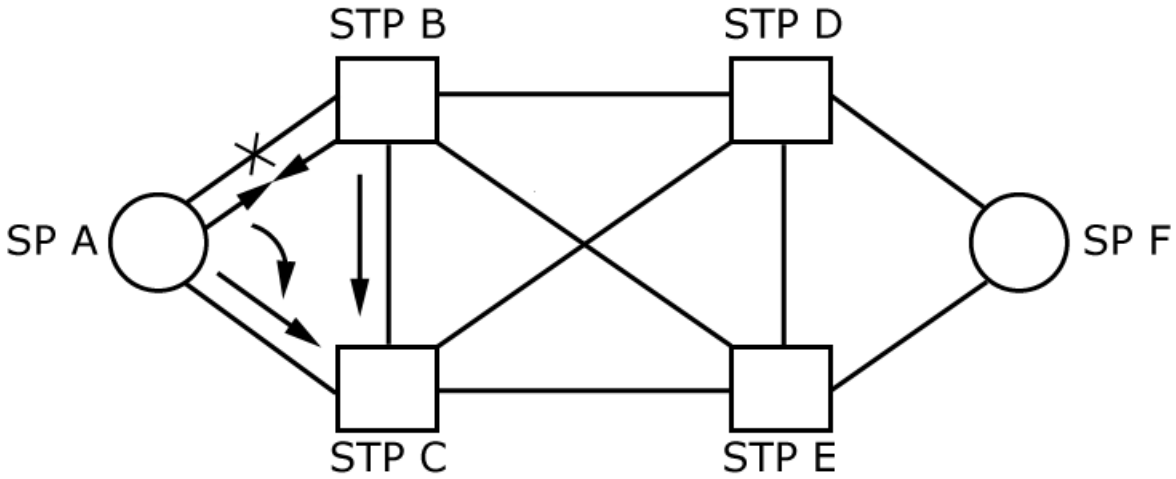


Рис. 19.6. Отказ звена сигнализации

19.3.1. Алгоритм при отказе звена сигнализации

При отказе звена (AB) между исходящим и транзитным пунктами сигнализации предпринимаются следующие действия (рис. 19.6):

- в соответствии с данными таблицы 17.1 (глава 17) пункт A переводит трафик звена AB на звено AC, а пункт B переводит трафик звена BA на звено BC. Перевод трафика производится с помощью процедуры перехода на резервное сигнальное звено и предусматривает обмен сообщениями COO и COA через транзитный пункт C (см. рис. 19.1, б). После завершения считывания сообщений из буфера звена AB и переноса их в буфер передачи звена AC в пункте A производится перезапуск трафика по звену AC; аналогичные действия производятся и в пункте B. Маршрут переноса сообщения из A в F удлиняется и проходит теперь через три транзитных пункта;
- кроме того, пункт B передает к пункту C сообщение запрещения переноса TFP относительно пункта назначения A (см. рис. 19.2);
- после приема сообщения TFP пункт C начинает периодически передавать к пункту B сообщения тестирования пучка сигнальных маршрутов RST относительно пункта назначения A (см. рис. 19.5).

19.3.2. Восстановление звена сигнализации

При восстановлении звена (AB) между исходящим и транзитным пунктами сигнализации предпринимаются следующие действия:

- пункт B инициирует процедуру возврата на нормальное звено, передавая пункту A через пункт C сообщение CBD с идентификатором звена AB. При приеме подтверждения CBA от пункта C в пункте B производится перезапуск сигнального трафика по звену AB. Кроме того, со стороны пункта B к пункту C передается сообщение TFA относительно пункта назначения A, т.е. TFA(A), после приема которого пункт C останавливает передачу сообщений SRT к пункту B.

19.4. Пример отказа и восстановления транзитного пункта сигнализации

Приведем алгоритм обмена сообщениями управления сетью сигнализации при отказе транзитного пункта сигнализации, а также алгоритм при его восстановлении. Рассмотрению подлежит участок сети ОКС№7, приведенный на рис. 19.7.

19.4.1. Отказ транзитного пункта сигнализации

При отказе транзитного пункта сигнализации D предпринимаются следующие действия (рис. 19.7):

- в пункте сигнализации B, Си F инициируется процедура перехода с блокированных звеньев BD, CD и FD на резервные звенья первого приоритета BE, CE и FE соответственно. Пункты B,C и D отправляют сообщения COO в пункт D через пункт E о переключении соответствующих ЗС. По причине отказа пункта D вышеуказанные пункты не получат ответных сообщений COA и произведут перезапуск трафика (как показано на рис. 19.7) по истечении выдержки времени T2=0,2-2сек. Кроме того, пункт E передает сообщения запрещения переноса TFP в пункты B, C и F относительно пункта D. При приеме TFP пункты B, C и F начинают передавать к пункту E сообщения тестирования пучка сигнальных маршрутов к пункту D, т.е. RST (см. рис. 19.5);
- в пункте B после приема от пункта E сообщения TFP относительно D производится обновление маршрутных таблиц с целью отклонения трафика, направляемого к D, вследствие чего к пункту C передается сообщение TFP относительно пункта D. Аналогичные действия производятся в пункте C, который передает сообщение TFP к B;
- получив от C сообщение TFP, пункт B отмечает пункт назначения D как недоступный и передает сообщение TFP к пункту A. Аналогичные действия производятся в пункте C, который передает сообщение TFP к пункту A. Приняв сообщения TFP от пунктов B и C, пункт A определяет, что пункт назначения D стал недосягаем, и останавливает передачу к нему сигнального трафика;
- аналогичным образом, передачей от звена к звену сообщений TFP относительно отказавшего пункта D, пункты A и E оповещаются о его недосягаемости и начинают тестирование пучков маршрутов в его направлении через соответствующие смежные пункты.

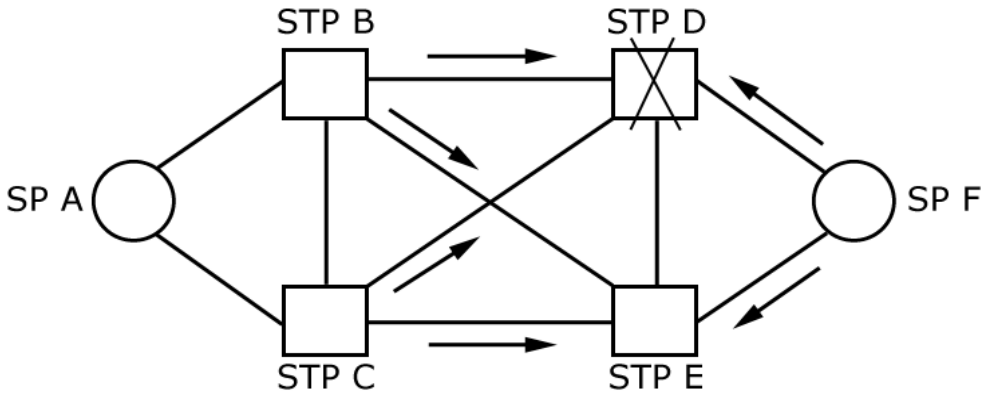


Рис. 19.7. Отказ транзитного пункта сигнализации D

19.4.2. Восстановление транзитного пункта

При восстановлении транзитного пункта D предпринимаются следующие действия:

- определив досягаемость пункта D, пункты сигнализации B, C и F передают к нему сообщения разрешения перезапуска трафика TRA (см. рис. 19.3, б);
- при срабатывании или остановке таймера T20 транзитный пункт D рассылает сообщения TRA всем смежным пунктам (см. рис. 19.3, г);
- в пунктах B, C и F выполняются контролируемые выдержкой времени T4 и T5 (см. разд.19.1.1) процедуры возврата с резервных на исходные (нормальные звенья). Контроль выдержкой времени используется по той причине, что пункт D все еще недосягаем через E в пунктах B, C и F в результате ранее принятых от него сообщений запрещения переноса TFP;
- пункт E передает к пунктам B, C и F сообщения разрешения переноса TFA относительно пункта назначения D, при приеме которых пункты B, C и F, в свою очередь, направляют сообщения TFA к смежным с ними пунктами. Передачей сообщений TFA от звена к звену производится оповещение всех пунктов о том, что пункт D стал доступным;
- при приеме сообщений TFA в каждом из пунктов прекращается передача сообщений тестирования RST пучка маршрутов относительно пункта D;
- в пунктах B, C и F производится перезапуск трафика, который в нормальных условиях передается через транзитный пункт D.

ГЛАВА 20. Интеллектуальные сети

20.1. Принцип обслуживания вызовов в сети ТфОП/ISDN на основе интеллектуальной сети

Технология сети ISDN, обеспечивающая 22 услуги связи (конференцсвязь, переадресация, удержание соединения и др.), имеет следующий недостаток. Введение новых услуг связи, спрос на которые в условиях рыночной экономики растет, связан с проблемами модернизации программного обеспечения в станции коммутации. Новая технология интеллектуальной сети связи IN (Intelligent Network) позволяет разделить функции обработки основного вызова на соединение от функций предоставления услуг. Этот принцип позволяет также вводить новые услуги связи в программном обеспечении, не входящем в узел коммутации [61,62]. На рис. 20.1 показан принцип обслуживания вызовов в сети ТфОП/ISDN на основе интеллектуальной сети.

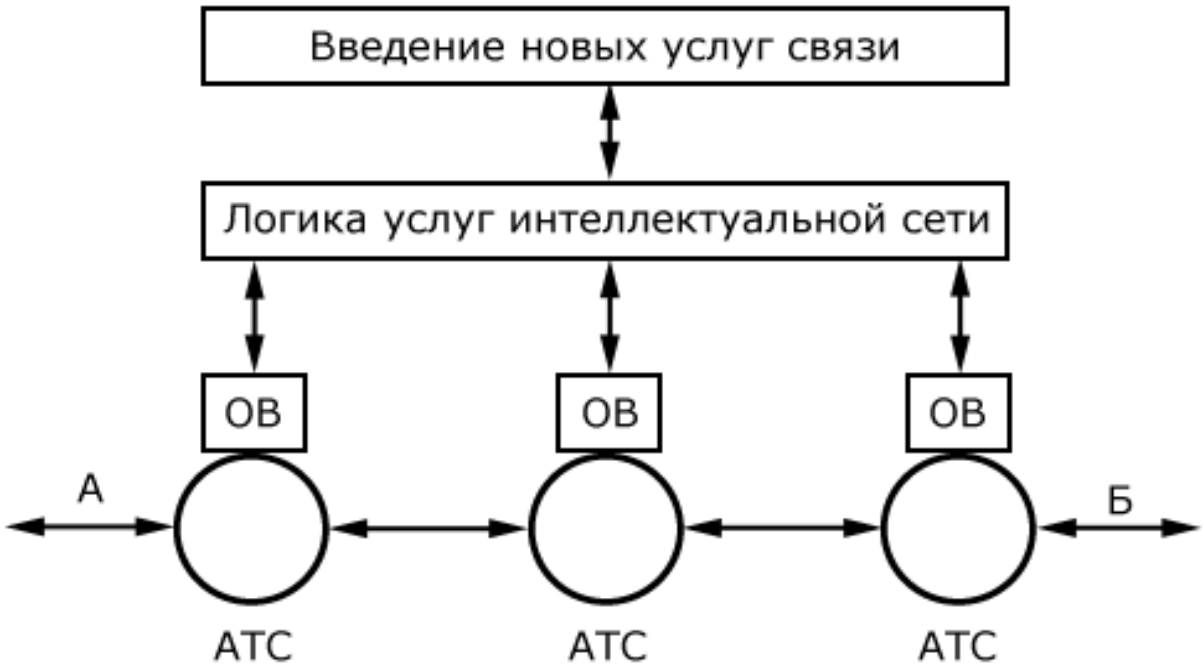


Рис. 20.1. Обслуживание вызовов в ТфОП/ISDN на основе IN

Модель обслуживания вызовов в IN включает:

- технические средства обработки основных вызовов, выполняющие функции вне зависимости от услуг;
- определители вызовов (ОВ), опознающие заявки в IN и временно приостанавливающие процессы обслуживания вызовов на период обмена информацией с логической частью IN;
- логическая часть для создания дополнительных услуг и для передачи информации, управляющей стандартными процессами обработки вызовов в соответствии с предоставляемой услугой.

Развитие интеллектуальных сетей в России началось с почти десятилетним отставанием от стран с развитыми сетями телекоммуникаций. Из стандартизованного набора услуг CS1 на российском рынке абонентам и пользователям предлагается ограниченный набор. Среди этого набора «Бесплатный вызов» (или услуга «800») является наиболее востребованной услугой. Изложим логику работы IN на примере этой услуги в сети ТфОП/ISDN. На рис. 20.2 приведена схема упрощенного алгоритма взаимодействия устройств при предоставлении услуги «800» (Бесплатный вызов).

Обозначения на схеме:

- SSP - узел коммутации услуг (Service Switch Point);
- SCP – узел управления услугами (Service Control Point);
- IP – интеллектуальное периферийное устройство (Intellectual Peripheral);
- SDP – узел базы данных (Service Data Point).

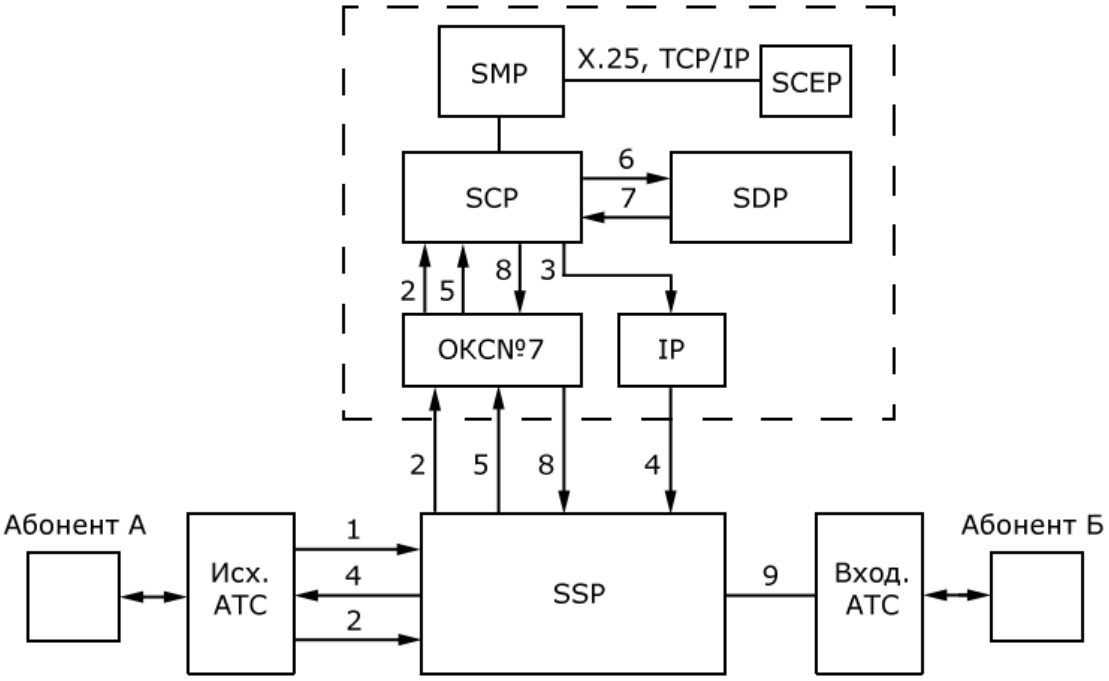


Рис. 20.2. Алгоритм взаимодействия устройств при предоставлении услуги «800» (Бесплатный вызов)

Рассмотрим алгоритм предоставления услуги «800».

- Абонент набирает номер 8-800…, где 8- выход к платформе IN через АМТС (автоматическую междугороднюю станцию) 800 – код доступа к услуге

«800» (Бесплатный вызов), объявленный в рекламе номер, принадлежащий компании по заказу билетов;

- SSP приостанавливает процесс обслуживания телефонного вызова и транслирует код услуги в узел SCP через сеть ОКС№7;
- SCP, проанализировав код «800», дает команду устройству IP на передачу голосового сообщения о наборе номера абонента услуги «800»;
- IP выдает голосовое сообщение абоненту А о необходимости набора номера абонента услуги «800»;
- Абонент набирает объявленный в рекламе логический номер (например, компании по заказу авиабилетов – 3333333) и передает это сообщение ОКС№7 из SSP в SCP. При наличии вызываемого абонента Б в другой интеллектуальной платформе сообщение из SSP проходит к SCP по сети ОКС№7 через несколько транзитных пунктов сигнализации.

- SCP анализирует введенный логический номер и делает запрос в узел SDP для того, чтобы определить физический номер того филиала компании (абонента компании), который готов обслужить абонента А.
- SDP пересчитывает логический номер (3333333) в физический номер (например, 55555555) и передает его в SCP;
- SCP определяет номер счета абонента услуги (Б) и передает в SSP через ОКС №7 сообщение услуги «800» прикладного протокола пользователя INAP (Inelligent Network Application Part) об организации начисления оплаты и о физическом номере абонента услуги;
- SSP возобновляет приостановленный ранее процесс обслуживания вызова, передает номер абонента Б во входящую АТС и проключает соединительный тракт между абонентом А и абонентом Б. На рис. 20.2 приведены остальные два узла IN (SMP и SCEP), которые вместе с SCP составляют платформу интеллектуальной сети.

SCEP - пункт создания новых услуг (Service Creation Environment Point);
SMP – пункт административного управления, выполняющий функции по системам расчетов с абонентом, вводу новых услуг, техобслуживания (Service Management Point).
На ТфОП РФ SSP устанавливается либо непосредственно на АМТС, либо является выделенным элементом.
Интеллектуальная периферия (автоинформаторы, автоответчики и.т.д.) информирует абонента при предоставлении ему услуги IN. Интеллектуальная периферия используется в РФ в интегрированном варианте с оборудованием SSP.

20.2. Подсистема SCCP в стеке протоколов ОКС№7 интеллектуальной сети

Подсистема передачи сообщений MTP обеспечивает реализацию в полной степени только функций уровней 1 и 2 эталонной модели OSI. Для реализации всех функций уровня 3 модели OSI потребовалось ввести в систему ОКС№7 дополнительную подсистему управления соединением сигнализации SCCP. Одна из причин внедрения SCCP рассмотренная ранее необходимость в ISDN сигнализации «из конца в конец». Это не единственная и не основная причина необходимости SCCP. В других случаях также важно передавать сообщения безотносительно к установлению информационного канала между пользователями. Примером является приведённый обмен сообщениями на рис. 2 между SCP и SSP при предоставлении услуги «800» интеллектуальной сети.
На рис. 20.3 приведён стек протоколов ОКС№7 в интеллектуальной сети. INAP является

прикладным протоколом пользователя интеллектуальной сети, который обеспечивает необходимые функции и процедуры системы ОКС№7 в интеллектуальной сети. TCAP (Transaction Capability Application Part) является прикладной подсистемой возможностей транзакций и обеспечивает интерфейс необходимого протокола пользователя (в данном случае протокола INAP) и его взаимодействие с SCCP.

Подсистема MTP предназначена только для передачи информации, связанной с установлением информационного канала. Подсистема управления сигнальным соединением SCCP даёт возможность установления соединений сигнализации безотносительно к установлению информационного канала между пользователями.

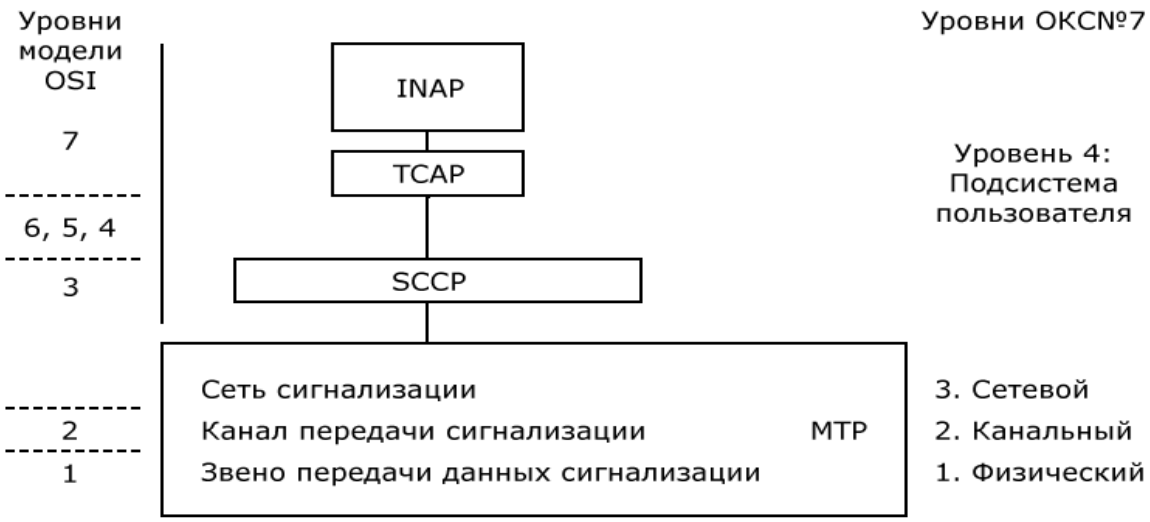


Рис. 20.3. Стек протоколов системы ОКС№7 в интеллектуальной сети

Подсистема SCCP выполняет следующие дополнительные возможности при работе через подсистему MTP:

- расширяет функции сетевого уровня подсистемы MTP - третьего уровня модели OSI;
- обеспечивает работу служб передачи данных без установления соединения и служб с установлением соединений;
- обеспечивает гибкие механизмы управления маршрутизацией;
- обеспечивает управление подсистемой SCCP;
- осуществляет расширение адресации.

Подсистема управления соединением сигнализации SCCP состоит из следующих функциональных блоков.

- служба передачи сообщений с установлением и без установления соединения;
- управление маршрутизацией SCCP (SCRC, SCCP Routing Control);
- управление подсистемой SCCP (SCMG, SCCP Management).

20.2.1. Службы передачи сообщений

Подсистема SCCP предоставляет две категории служб для передачи сообщений: без установления соединений и с установлением соединений. На рис. 20.4 приведена диаграмма обмена информацией SCCP без установления соединения. Для обмена информацией без установления соединения используются только два типа сообщений - UDT (Unit Data) и UDTS (Unit Data Service).

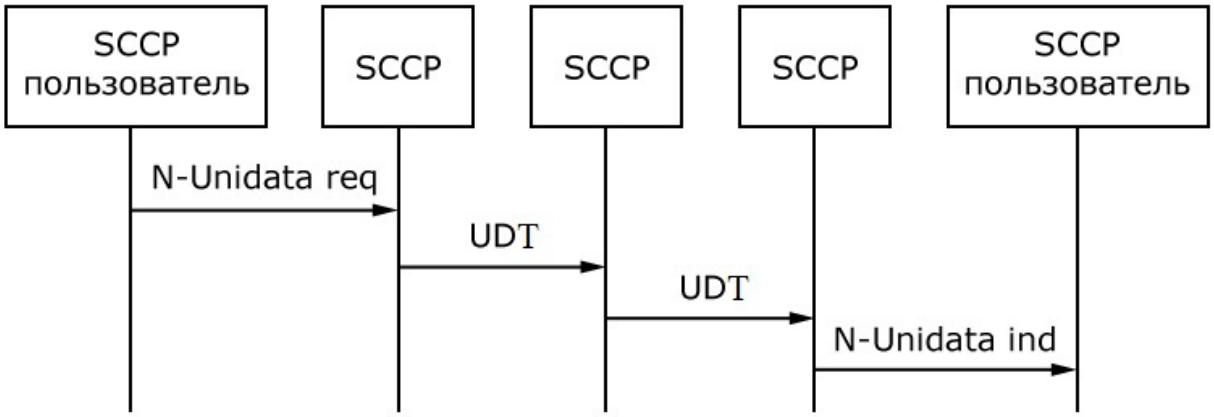


Рис. 20.4. Диаграмма обмена информацией SCCP без установления соединения

Формат сообщения UDT включает адреса вызывающего SP и вызываемого SP, а также поле «данные». Полученное передающим SP сообщение UDTS информирует о том, что сообщение UDT не принято в пункте назначения. В формате UDTS к указанным полям UDT включено дополнительное поле причины возврата. На рис. 20.5. приведена диаграмма обмена информацией SCCP с установлением соединения. Здесь введены следующие обозначения:

- CR- сообщение SCCP «запрос соединения».
- CC- сообщение SCCP «подтверждение соединения».
- DT- сообщение «данные».
- АК - подтверждение приема данных.

В каждое из этих сообщений входит поле параметра «местный условный номер», являющийся идентификатором канала.

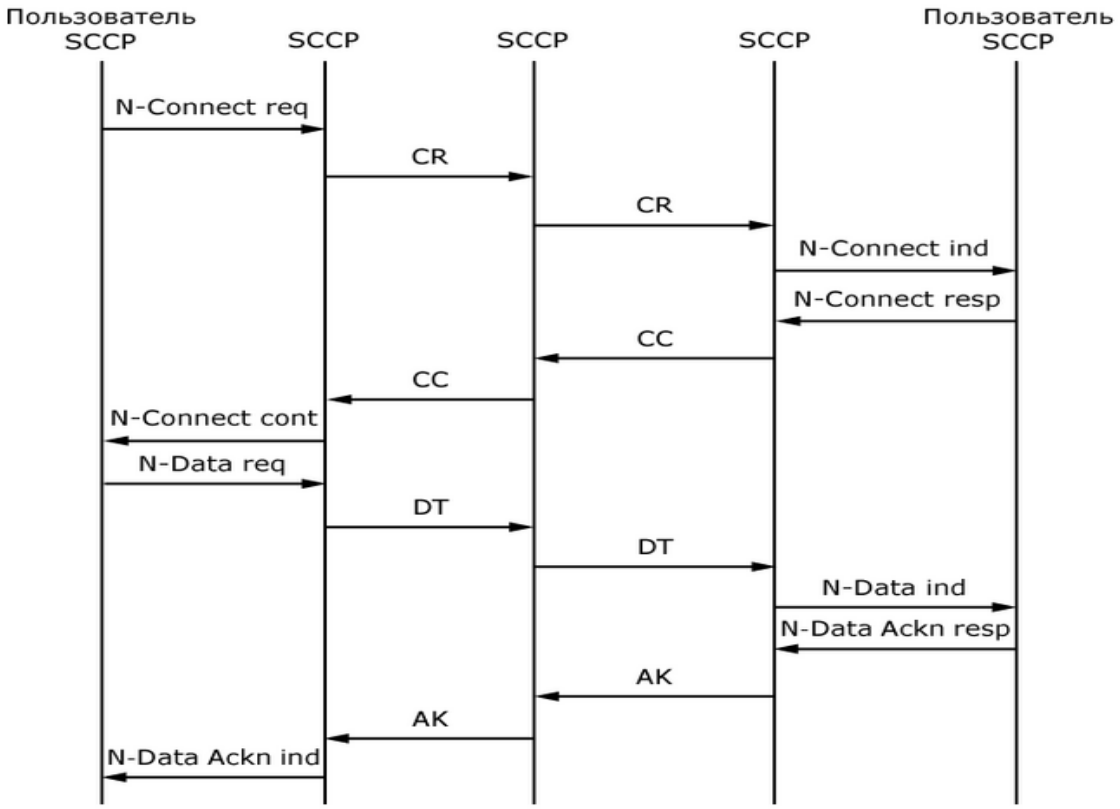


Рис. 20.5. Диаграмма обмена информацией SCCP с установлением соединения

20.2.2. Управление маршрутизацией

Управление маршрутизацией SCCP (SCRC, SCCP Routing Control) вносит дополнения к маршрутизации подсистемы MTP3. Адресация кодов пунктов сигнализации OPC и DPC обеспечивает доставку сообщений в узел, но не указывает на конкретный вид услуги, передаваемой в этом сообщении. SCCP дополняет адресацию MTP номером подсистемы SSN (Subsystem Number), который указывает в случае IN на конкретную услугу в данном узле. Комбинация OPC + SSN является в этом случае адресом вызывающей стороны, а DPC + SSN - адресом вызываемой стороны. Согласно рекомендации ITU-T для услуги «800» IN определён SSN = «11111110», для услуги автоматической службы предоплаченных карт — 11111101, а для услуги «Виртуальная частная сеть» - «11111100».

Подсистема SCCP поддерживает также маршрутизацию по глобальным заголовкам GT (Global Title). Глобальный заголовок представляет собой адрес, не содержащий явной

информации о маршруте к узлу ОКС№7, т.е. DPC и SSN. Это может быть в интеллектуальной сети номер 800-й серии услуг IN и телефонный адрес согласно стандарту E.164. Трансляция глобального заголовка используется для освобождения пунктов сигнализации от необходимости хранения информации о каждом приложении получателя (т.е. код DPC+SSN). Например, запросы к телефонной карточке (которые используются для проверки того, что с ее помощью можно должным образом оплатить услуги) должны быть направлены к пункту управления услугами SCP производителя карточки. Вместо того чтобы такой запрос обрабатывался централизованной национальной базой данных, SCP генерирует запрос локальному STP, который в результате трансляции глобального заголовка с помощью своей базы данных выбирает получателя этого запроса. Использование трансляции глобального заголовка минимизирует необходимость хранения в передающем пункте сигнализации информации о далеко удаленных от него узлах. Трансляция глобального заголовка используется также для распределения нагрузки между SCP или в случае их отказов. В этих примерах, когда сообщения достигают конечного пункта сигнализации для финальной трансляции заголовка и маршрутизации к получателю, этот пункт сигнализации может принять решение: выбрать один их двух сопряженных с ним пунктов в зависимости от их работоспособности, нагрузки, приоритета или выбрать оба при распределении нагрузки. Когда коммутатор запрашивает трансляцию, он должен определить лишь характер необходимой транзакции (например, логический номер преобразовать в «реальный» номер формата E.164) и отправить запрос к узлу, который поддерживает соответствующую таблицу маршрутизации.

20.2.3. Управление подсистемой SCCP

Система управления подсистемой SCCP, обозначаемая SCMG (SCCP Management) поддерживает функцию отслеживания состояния удалённого SCCP-пункта, а также локальных подсистем (т.е. в интеллектуальной сети узлов SSP, SCP, а также блоков обеспечения услуг). В определенной степени управление подсистемой SCCP похоже на функции управления сетью сигнализации на уровне MTP3. Система управления SCMG позволяет поток данных подсистемы SCCP не направлять к недоступному получателю, обеспечивает возможность направлять его по резервному маршруту, ограничивать поток при перегрузке сети. Система SCMG взаимодействует с системой управления маршрутизацией SCRC. Система SCMG использует концепцию «заинтересованной» подсистемы или сигнального пункта, которые требуют уведомления после изменения состояния интересующего их пункта сигнализации. В случае сбоя или неработоспособности узла

«заинтересованным» узлам направляется широковещательное сообщение - SSP о ее недоступности (Subsystem Prohibited). Уведомленный пункт сигнализации или подсистема может периодически проверять доступность системы, отправляя периодически сообщения проверки состояния подсистемы SST (Subsystem ctatus Test) к заданному пункту. Если подсистема готова к работе, то отправляется сообщение о работоспособности подсистемы SSA (Subsystem Allowed).

Ниже приведем еще несколько сообщений системы управления подсистемой SCCP, которые так же, как и вышеописанные сообщения (SSP, SST, SSA) не зависят от приведенных в предыдущей главе сообщений управления сетью сигнализации на уровне MTP3:

- SSC (SCCP/Subsystem Congested). Перегруженность протоколов/подсистемы SCCP.
- SOR (Subsystem Out-of-Service Request). Используется для передачи запроса перехода на дублирующую систему.
- SOG (Subsystem Out-of-Service -grant). Используется в качестве ответа на SOR согласием на резервирование.

20.2.4. Расширение адресации

SCCP используется для расширения адресации пунктов сигнализации. В число объектов, требующих наличия кода пункта сигнализации (OPC и DPC), входят не только узлы коммутации SSP и SCP интеллектуальной сети, станции коммутации ТфОП/ISDN, но и узлы сотовых сетей подвижной связи GSM (использование ОКС№7 в GSM рассматривается в следующих главах). Единая сеть электросвязи России относится к одной из крупнейших сетей в мире, поэтому поля в 14 бит для кода OPC / DPC может оказаться недостаточно общее число пунктов сигнализации 2^{14}=16384.

Для решения этого вопроса надо было либо отводить под это поле 24 бита этикетки (как принято в США), либо строить сеть по иерархическому способу, оставив поле 14 бит. Было принято второе решение.

20.3. Взаимодействие уровней ОКС №7 в сети IN. Пример алгоритма представления услуги

На рис. 20.6 показано взаимодействие уровней ОКС№7 в интеллектуальной сети. Здесь видно, что между прикладным уровнем интеллектуальной сети INAP и подсистемой SCCP введён прикладной уровень подсистемы возможностей трансляции TCAP. Назначение TCAP предоставить шлюз для передачи между пунктами сигнализации ОКС№7 сообщений между

прикладным уровнем и уровнем SCCP независимо от подсистемы пользователя (INAP, прикладной уровень мобильных сетей - MAP и др.).

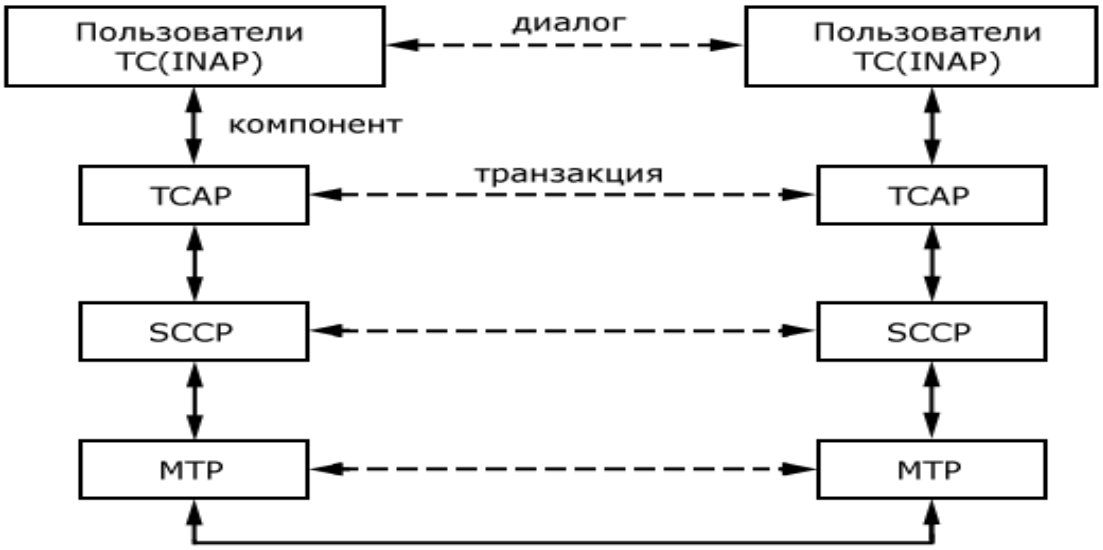


Рис. 20.6. Взаимодействие уровней ОКС №7 в сети IN

Здесь используются следующие термины и определения:

- Пользователи ТС (Transaction Capability, пользователи возможности транзакций) – прикладной процесс, использующий TCAP как протокол с сетью. В случае IN это прикладной протокол INAP (в мобильных сетях связи – MAP; в системе эксплуатации, технического обслуживания и администрирования сети ОКС№7 – OMAP).

- Транзакция – логическая связь между двумя TCAP для реализации передачи данных пользователей ТС.
- Компанент – единица данных протокола для обмена между двумя пользователями ТС.
- Диалог – логическая связь, устанавливаемая между пользователями ТС для обмена компонентами.

Рассмотрим использование протокола INAP и TCAP на примере предоставления услуги с дополнительной оплатой PRM (Premium Rate) [63]. Эта услуга реализована в ЕСЭ России. Суть услуги PRM состоит в том, что за предоставление по телефону медицинской, юридической или другой консультации телефонная компания берет дополнительную плату.

Затем эта компания рассчитывается с поставщиком услуги или выписывает счет пользователю услуги от имени поставщика услуг. Эта услуга, также как и услуга «800» является наиболее широко используемой в России.

Рис. 20.7 иллюстрирует упрощённую схему предоставления услуги PRM. А-пользователь набирает номер 8-xxx-7-1234, тем самым по коду «8» он выходит на междугородную сеть, а по коду «xxx» выходит на ту АТМС, которая выполняет функции SSP; «7» означает код услуги PRM, а 1234 – номер услуги PRM (например, медицинская консультации по детским заболеваниям). SCP сообщает в SSP – кто, сколько должен платить за предоставление услуги (т.е. как формировать запись об услуге) и сообщает номер В-пользователя (в нашем случае – дежурного детского врача), который окажет требуемую услугу. Услуга «7» — это один из номеров серии 8xxx (для услуги PRM – это 8905).

Подключение по международному коду абонента одной зоны к интеллектуальной платформе другой зоны страны позволяет предоставить услуги IN удаленному абоненту. После распознавания кода услуги «7» станция SSP инициирует сеанс связи с SCP, т.е. готовит сообщение INAP о запросе услуги в виде сообщения InitialDP (Initial Detection Point – начальная точка обнаружения) и передает его посредством протокола подсистемы транзакций TCAP в виде TC_Begin (InitialDP). SSP получает ответ из SCP, в котором содержится информация, как произвести расчет за услугу (в операции FCI, Furnish Charging Information), а также адрес В-пользователя в операции CONNECT. На этом использование SCP кончается.

В действительности, процесс несколько сложнее – следует еще ответное сообщение о возможных ошибках и команда TC_End, но главное – должны быть два основных свойства услуги PRM:

- пересчет кода и номера услуги в адрес В-пользователя;
- определение размера и адресата оплаты и распределение оплаты между оператором связи и абонентом услуги (в нашем случае – врачом педиатором).

А- пользователь В-пользователь

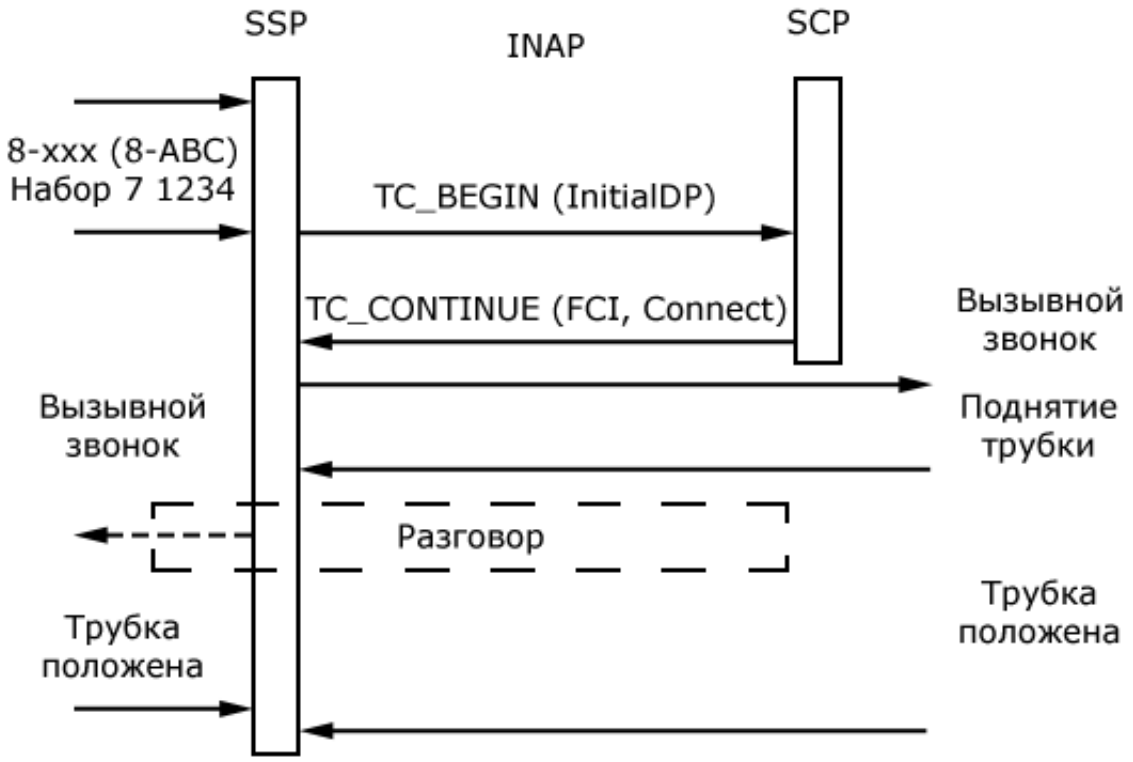


Рис 20.7. Схема предоставления услуги PRM

На рис. 20.8 приведена архитектура протокола INAP при взаимодействии SCP и SSP. Протокол INAP представлен набором из подпротоколов ASE (Application Service Element) выполнения отдельных операций. В свою очередь, каждый ASE опирается на подсистему транзакций TCAP, т.е. подпротоколы ASE являются пользователями TC. Коммутатор услуг SSP реализует три функции:

- коммутацию услуги SSF, выполняющую переключение к SCP при обнаружении запроса на интеллектуальную услугу;
- установление соединения через данную АТС (CCF);
- специализированных ресурсов SRF (Specialized Resource Function), т.е. функцию интеллектуальной периферии.

Узел управления услугами SCP реализует функцию управления услугой SCF, т.е. управление прохождением алгоритма услуги согласно протоколу. Например, если SSF получает примитив-индикацию запроса услуги DP (Detection Point), то формируется сообщение, которое называется операцией Initial DP Operation (рис. 20.7). Посредством подсистемы транзакций TCAP начинается сеанс связи с соответствующим уровнями

протоколов SCP. При этом используются также подсистемы SCCP, MTP сети ОКС№7.

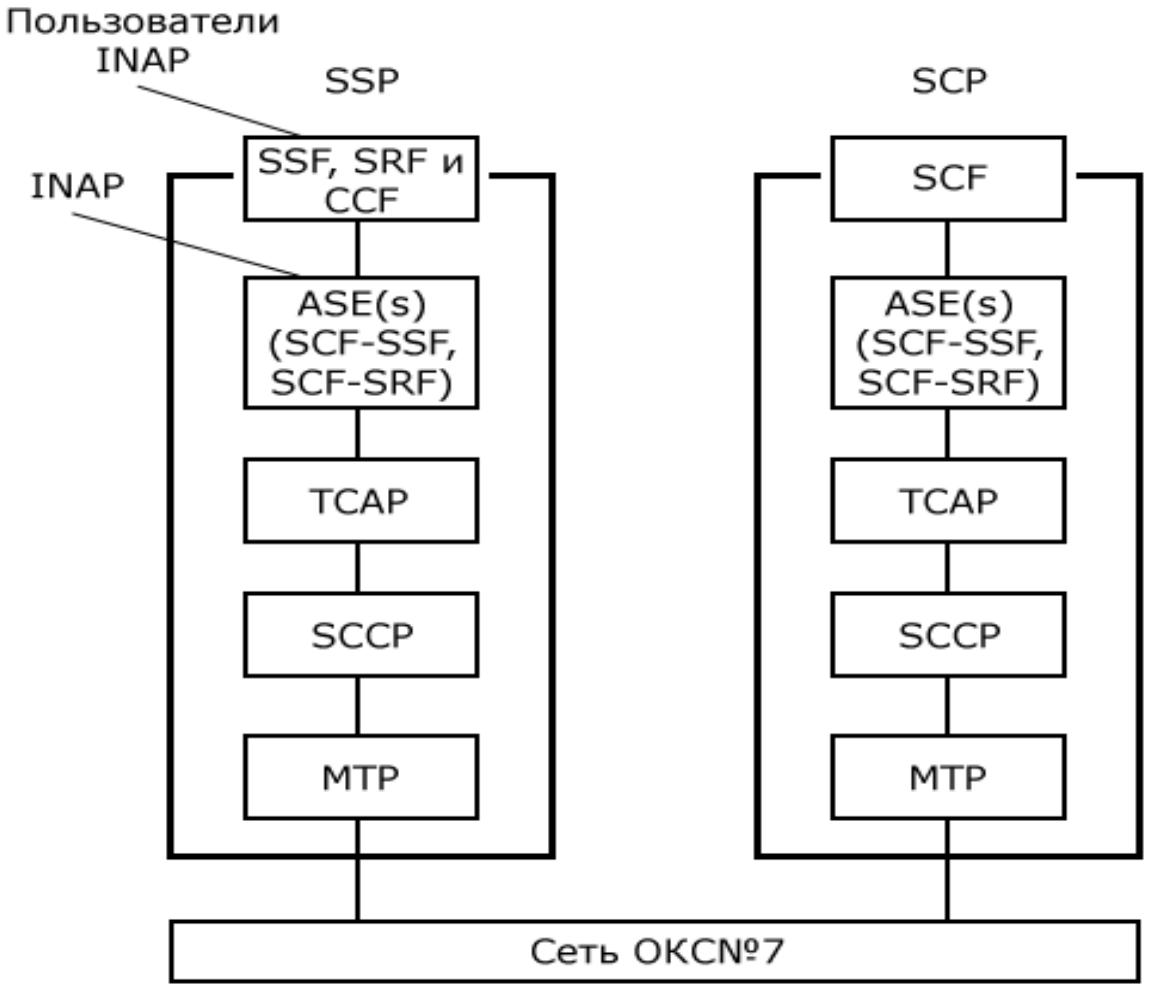


Рис. 20.8. Архитектура протокола INAP при взаимодействии SSP и SCP

20.4. Алгоритм аутентификации в протоколе услуги «универсальная персональная связь» интеллектуальной сети

Услуга «универсальная персональная связь» UPT (Universal Personal Telecommunication) относится к первому набору услуг CS (Capability Set) интеллектуальной сети. Эта услуга позволяет абоненту пользоваться входящей и исходящей связью по единому номеру при его перемещении вне зависимости от сетевой инфраструктуры и местоположения. Для этой услуги важной задачей является обеспечение ИБ в части аутентификации абонента-роумера, т.е. не находящегося в сети приписки.

Аутентификация пользователя UPT сети IN построена на основе протокола ОКЛИК-ОТЗЫВ (приложение Г) и протокола Нидхема-Шредера [10], использующих шифрование с общим

ключом. На рис. 20.9 приведена четырехпроходная схема аутентификации абонента - роумера услуги UDP сети IN [64]. Под роумером понимается временное нахождение абонента в области сети, к которой он не приписан.

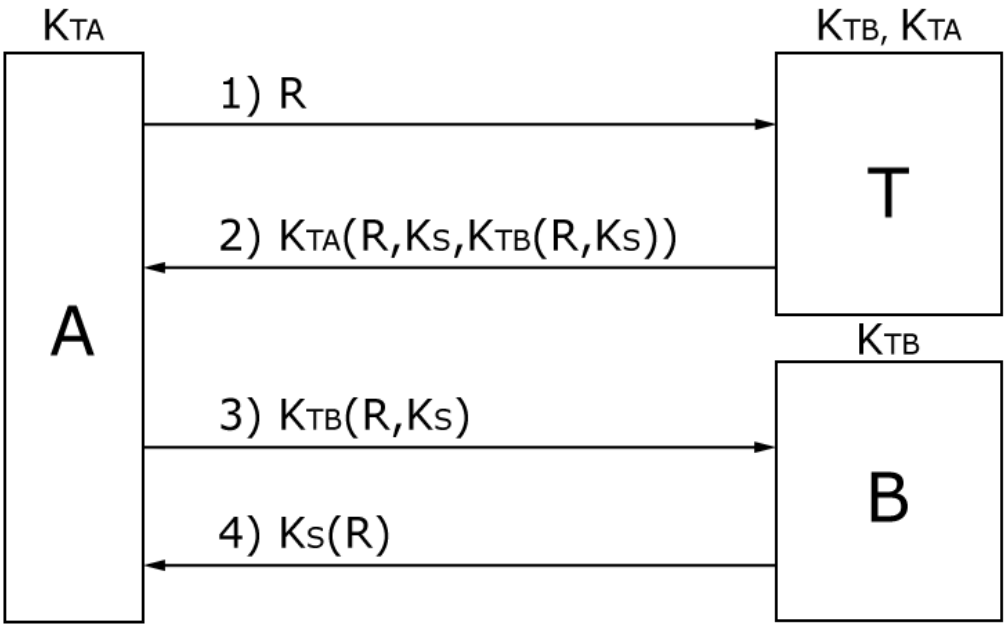


Рис. 20.9. Четырехпроходная аутентификация роумера B услуги UPT в сети IN

Аутентифицирующую функцию выполняет гостевая UPT система A, в которой находятся прибор UPT B. Домашняя UPT (система T) к которой приписан пользователь B, имеет общий секретный ключ K_{TB} с пользователем B и K_{TA} с гостевой UPT системой A. Из гостевой системы UPT A в адрес домашней UPT системы T передается случайное число R - оклик (сообщение 1). Домашний UPT (система T) генерирует ключ сеанса K_S , билет (квитанцию) доступа A к B (т.е. K_{TB} (R, K_S)) и шифрует оба эти сообщения общим ключом симметричного шифрования с гостевой UPT системой K_{TA}. Сообщение 2 передается из домашней UPT системы T в гостевую UPT систему A. Расшифровав сообщение 2 и определив R, гостевая UPT система убеждается в подлинности домашней UPT системы T. В сообщении 3 гостевая UPT отправляет квитанцию доступа K_{TB} (R, K_S) роумеру B.

Расшифровав это сообщение, роумер B отправляет гостевому UPT A зашифрованное ключом K_S случайное число R (сообщение 4). После расшифрования R в случае совпадения его со сгенерированном R перед отправлением его в сообщении 1 гостевая UPT A убеждается в подлинности пользователя-роумера B. Случайное число R служит для защиты от угрозы «повтор».

На рис. 20.10 приведена пятипроходная схема взаимной аутентификации абонента-роумера (B) и гостевой системы (A) услуги UPT интеллектуальной сети.

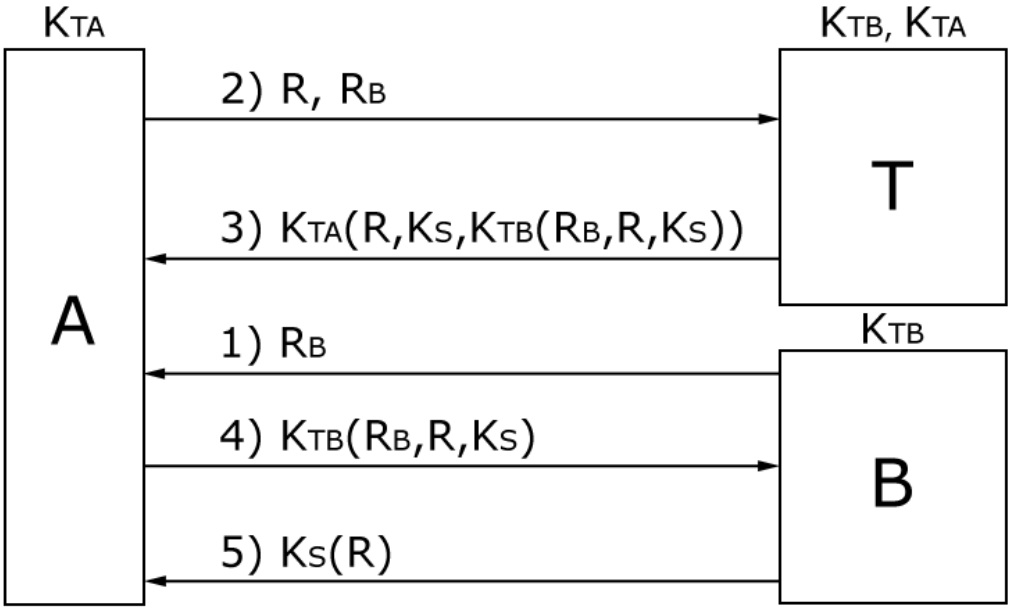


Рис. 20.10. Пятипроходная взаимная аутентификация абонента-роумера и гостевой UPT-системы

В сообщении 1 пользователь-роумер В услуги UPT отправляет случайное число (оклик) R_B в гостевую UPT систему А. Гостевая UPT система транслирует в домашнюю UPT систему Т этот оклик, а также передает сгенерированный оклик R (сообщение 2). Из домашней UPT системы в гостевую UPT систему сообщение 3 передается $K_{TA}(R,K_S,K_{TB}(R_B,R,K_S))$.

Сообщение 3 зашифровано общим ключом K_{TA} домашней и гостевой систем UPT. Это сообщение включает:

- квитанцию $K_{TB}(R_B,R,K_S)$ доступа к роумеру В. Здесь K_S является сеансовым ключом, сгенерированным в домашней UPT системе;
- случайное число R (оклик);
- сеансовый ключ K_S.

Сообщение 3 расшифровывается в гостевой UPT системе А ключом K_{TB}. Полученное случайное число R подтверждает подлинность домашней UPT системы Т. Гостевая UPT система транслирует квитанцию пользователю-роумеру (сообщение 4). Роумер расшифровывает полученную квитанцию, получает R_B и сравнивает с R_B, отправленным в сообщении 1. Совпадение этих значений подтверждает подлинность гостевой UPT системы.

Пользователь-роумер В отправляет случайное число R, зашифрованное ключом K_S (ключ K_S расшифровывается при приеме сообщения 4) в гостевую UPT систему А (сообщение 5). Расшифрованное сеансовым ключом K_S значение R позволяет убедиться в подлинности пользователя-роумера услуги UPT.

20.5. Количественная оценка угроз безопасности интеллектуальной сети

В документах ETSI изложены предложения по количественной оценке угрозы информационной безопасности отдельно для всей (глобальной) интеллектуальной сети и для одной из ее услуг — UPT.

Для глобальной IN угроза безопасности оценивается характеристикой чувствительности (sensitivity) [65]. Согласно терминологии ETSI [66] под чувствительностью понимается мера ценности, присвоенная информации для того, чтобы указать на необходимость в защите. Характеристика чувствительности относится не к конкретной угрозе, а к информации, подверженной воздействию нескольких угроз. Количественная характеристика оценивается тремя уровнями чувствительности:

- высоким, если информация содержит приватные или конфиденциальные данные;
- средним, если информация содержит адреса и данные по оплате;

- низкие, если информация относится к сбросу соединения.

Оценка чувствительности относится либо к конкретному сообщению прикладного уровня INAP, либо к потоку сообщений INAP между функциональными объектами. При проектировании информационной безопасности сетей связи следует провести анализ чувствительности отдельных потоков информации к конкретным угрозам. В работе [67] приводятся основные положения такого анализа на примере интеллектуальной сети связи. Метод количественной оценки каждой угрозы информационной безопасности ее услуги UPT предусматривает три характеристики, две из которых являются характеристиками документа ETSI ETR 320, приведенные в приложении А (раздел А3): вероятность реализации угрозы P и оценка последствий реализации угрозы G. В отличие от документа ETSI ETR 320 количественная оценка угрозы ранжируется экспертами не на основании произведения этих значений. Третья характеристика угрозы определяется сложностью реализации мер по защите, которая может принимать следующие значения:

0 — мера по защите от данной угрозы предусмотрены в сети;
1 — меры по защите от данной угрозы легко осуществимы;
2 — меры по защите от данной угрозы сложные;
3 — меры по защите от данной угрозы трудно осуществимы.

Для операторов сетей связи России, оборудование которых в течение долгого времени находится в эксплуатации, сложность реализации мер по защите от некоторых угроз безопасности может оказаться сложной или трудно осуществимой задачей.

ГЛАВА 21. Сети стандарта GSM

21.1. Классификация беспроводных сетей связи

Беспроводные сети позволяют связываться и получать доступ к приложениям и информации без использования проводных соединений. Существует большое количество разнообразных технологий беспроводных сетей, которые могут быть классифицированы в зависимости от размеров территориальной зоны, в которой они способны обеспечить связь. При этом они подразделяются на четыре основных типа (табл. 21.1):

- Беспроводная глобальная сеть WWAN (Wireless Wide Area Network);
- Беспроводная городская сеть WMAN (Wireless Metropolian Area Network);
- Беспроводная локальная сеть WLAN (Wireless Local Area Network);
- Беспроводная персональная сеть WPAN (Wireless Personal Area Network).

Таблица 21.1. Разновидности беспроводных сетей

Тип	Сфера действия	Стандарты
WWAN	По всему миру	Сотовые системы связи поколений 2, 2.5 и 3
WMAN	В пределах города	IEEE 802.16, WiMAX, IEEE 802.11s, mesh-сети
WLAN	В пределах зданий	IEEE 802.11, Wi-Fi
WPAN	В непосредственной близости от пользователя	IEEE 802.15, Bluetooth

Каждый узел беспроводной линии связи оснащается антенной, которая одновременно является передатчиком и приёмником электромагнитных волн. Электромагнитные волны распространяются в атмосфере со скоростью 300 тыс. км/с во все направления или в пределах определённого сектора. Беспроводная среда отличается высоким уровнем помех. Поскольку ресурсы радиочастот весьма ограничены, стоит задача общего всемирного регулирования использования частот. Для всемирной координации распределения частот мир был разделён Международной Союзом Электросвязи в области радиосвязи (МСЭ-Р) ITU-R (International Telecommunication Union-Radio Sector) на три региона. Комитет ITU-R периодически проводит конференции, на которых утверждается распределение частот во всех трёх регионах. В табл. 21.2 приведено несколько примеров частот, используемых в трёх регионах для WWAN и WLAN.

Таблица 21.2. Примеры распределения частот для беспроводных сетей

Тип сети	Сфера действия		
	Европа	США	Япония
WWAN	GSM 890 - 915 МГц 935 - 960 МГц 1710 - 1785 МГц 1805 - 1880 МГц	GSM 1850 – 1910 МГц 1930 - 1990 МГц	
WLAN	IEEE 802.11 2400 – 2483 МГц	IEEE 802.11 2400 – 2483 МГц	IEEE 802.11 2471 – 2497 МГц

На рис. 21.1 приведена упрощенная схема, иллюстрирующая распределение распространения сигналов в беспроводных сетях на три зоны – передача, детектирование и помехи.

Рис. 21.1. Зоны: передача, детектирование и помехи

В пределах зоны передачи передача возможна, т.е. приём сигнала осуществляется с достаточно малым количеством ошибок. В пределах зоны детектирования передаваемая мощность достаточно велика (выделяется из фонового шума). Однако для установления

связи количество ошибок оказывается слишком большим.

Внутри третьего (еще большего радиуса) передатчик фактически препятствует другим передачам, создавая фоновый шум. Приёмник не может детектировать посылаемые сигналы. Поэтому они лишь создают помехи другим сигналам. В реальности необходимо учитывать такое влияние условий распространения сигналов, как экранирование радиосигналов крупными препятствиями, отражение и рассеивание сигналов. Всё это, а также и многое другое является причиной многолучевого распространения сигнала [68].

Одним из следствий такого многолучевого распространения является более быстрое убывание интенсивности принимаемого сигнала. Этот эффект вызывает расширение начального сигнала из-за того, что распространяющиеся по различным путям сигналы достигнут антенны приёмника в разное время. Система GSM допускает расширения сигнала вследствие запаздывания до 16 мкс., т.е. более чем трёхкилометровую разность хода отдельных лучей. В результате отдельный импульс при приёме выглядит слабее других импульсов. Некоторые из принимаемых импульсов могут быть слишком слабы и проявляться в виде шума, т.е. происходит замирание и искажение результирующего сигнала.

Рассмотрим другой эффект от многолучевого распространения. Импульсы разных символов настолько отличаются по разности хода, что символы одного сигнала «налезают» на соседние символы другого. Этот эффект называется межсимвольной интерференцией. Чем выше скорость передачи, тем худшими будут последствия межсимвольной интерференции, так как предаваемые символы будут ближе друг к другу. Из-за этих помех накладываются ограничения на пропускную способность радиоканала.

Межсимвольная интерференция и расширение сигналов вследствие запаздывания имеют место даже в случае неподвижных передатчиков и приёмников. Ситуация ещё больше ухудшается, если передатчик и/или преемник находятся в движении.

21.2. Система GSM

Спектр радиоволн – это ограниченный ресурс. В отличие от проводного доступа, где у каждого терминала есть физическое соединение и связь с сетью, беспроводные системы обладают вполне определённым спектром частот, доступным в данном географическом регионе. Следовательно, от беспроводных сетей требуется тщательное выделение и распределение спектра в любом районе, чтобы множество пользователей могли одновременно устанавливать соединение. В настоящее время используются следующие способы использования спектра:

а) FDMA (Frequency Division Multiple Access) – множественный доступ с разделением каналов по частоте;

б) TDMA (Time Division Multiple Access) – множественный доступ с разделением каналов по времени;

в) CDMA (Code Division Multiple Access) – множественный доступ с кодовым разделением каналов;

г) OFDMA (Orthogonal Frequency Division Multiple Access) - ортогональный множественный досуп с частотным разделением.

Каждая из этих технологий разработана для того, чтобы обеспечить доступ к определенной частоте для многих пользователей (отсюда и множественный доступ во всех названиях). Глобальная система мобильной связи GSM (Global System for Mobile Communication) построена на основе множественного доступа FDMA и TDMA. Далее, глава 23 посвящена беспроводной сети связи стандарта 3G (UMTS), использующая доступ CDMA, и глава 25 - беспроводным сетям связи WiMAX и LTE, использующие доступ OFDMA.

21.2.1. Функциональная архитектура GSM

На рис. 21.2 приведена функциональная архитектура системы GSM, состоящая из трёх подсистем [69,70].

- Подсистема радиосвязи RSS (Radio SubSystem).
- Подсистема сетей и коммутации NSS (Network and Switching SubSystem).
- Операционная подсистема OSS(Operation SubSystem).

В интерфейсе A между подсистемами RSS и BSS используется система ИКМ-30 с коммутацией каналов 64 кбит/с. В интерфейсе O используется ОКС№7.

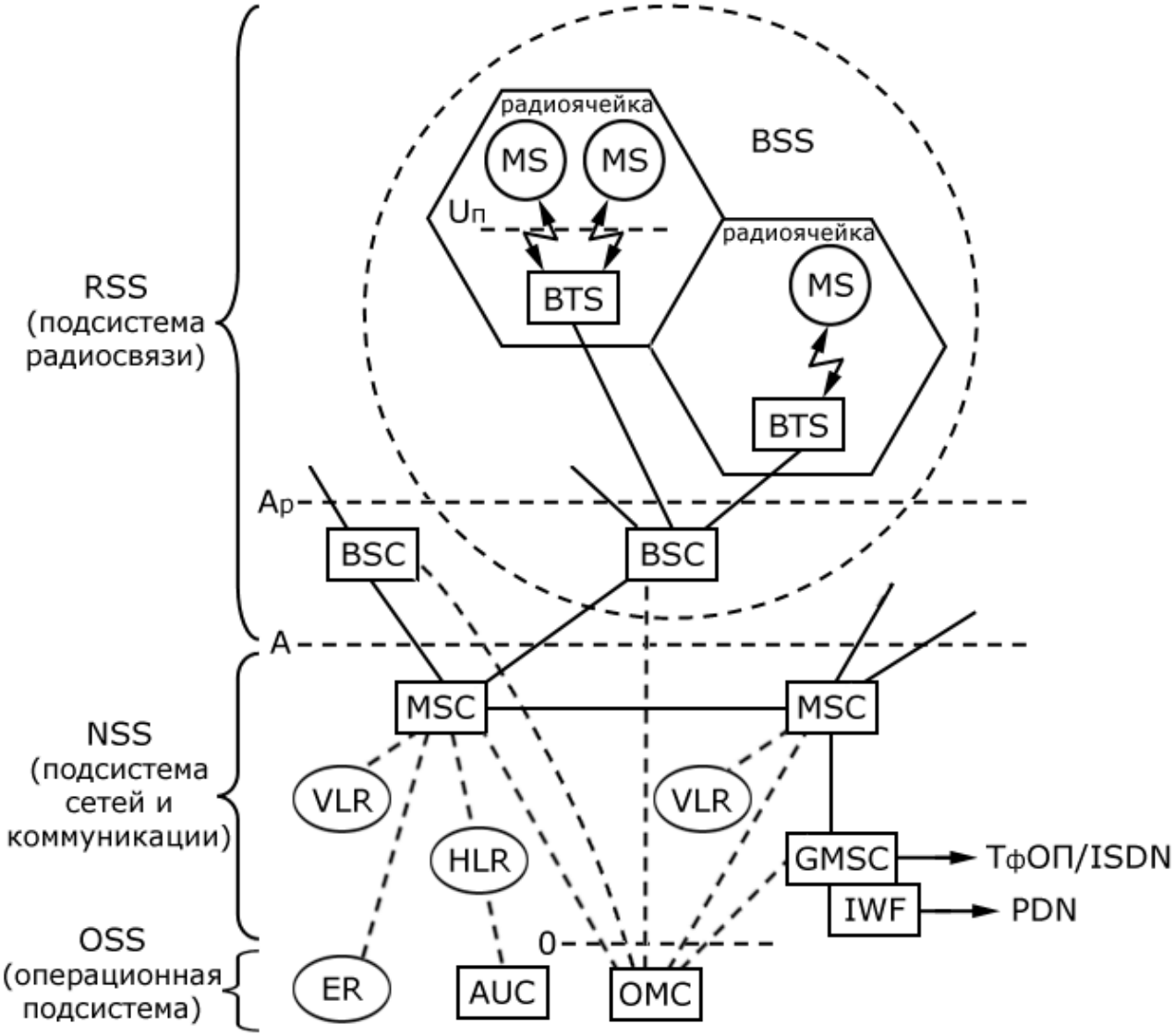


Рис. 21.2. Функциональная архитектура схемы GSM

21.2.1.1. Подсистема радиосвязи

Подсистема радиосвязи RSS включает оборудование, взаимодействующее на радиоучастке: мобильные станции MS (Mobile Station) и базовая станция BTS (Base Transceiver Station). Это оборудование составляет подсистему базовых станций BSS (Base Station System). Сеть GSM содержит много подсистем BSS. В состав MS входит всё пользовательское оборудование и программное обеспечение, необходимое для соединения. Описание мобильной станции MS приведено ниже. Пользователи GSM (мобильные станции MS) получают доступ к сети с помощью комбинации множественного доступа с частотным

разделением FDMA и множественного доступа с временным разделением TDMA. На рис. 21.3 показано каким образом это реализуется.

Между базовой станцией BTS, входящей в подсистему BSS, и мобильной станцией устанавливается дуплексный канал. Для каждого из двух направлений – от мобильной станции и наоборот используются различные частоты [10]. Одна из них используется для нисходящей линии связи (от BTS к MS), а другая – для восходящей линии связи (от MS к BTS). Системе GSM 900 выделено два диапазона частот по 25 МГц. Частотный диапазон от 890 до 915 МГц используется для восходящей линии, а от 935 до 960 МГц – для нисходящей линии связи. Оба диапазона разделены на 124 частотные полосы по 200 КГц каждая. На каждой частоте с использованием множественного доступа TDMA передаётся 8 каналов. Физическим каналом является временной слот, который передается на определенной частоте. Физические каналы организованы в пары. В каждую пару входит по одному физическому каналу для передачи в каждом направлении, несущие которых различаются на 45 МГц.

На рис. 21.3 восемь заштрихованных кадровых интервалов принадлежат одному и тому же соединению, по четыре в каждом направлении. Прием и передача происходит в разных интервалах. Если мобильной станции присвоен диапазон 890,2/935,2 МГц и кадровый интервал 2 хочет осуществить передачу на базовую станцию, он воспользуется нижним набором заштрихованных интервалов (а также последующими), размещая в каждом из них порцию данных. Так будет продолжаться до тех пор, пока не будут посланы все данные соединения.

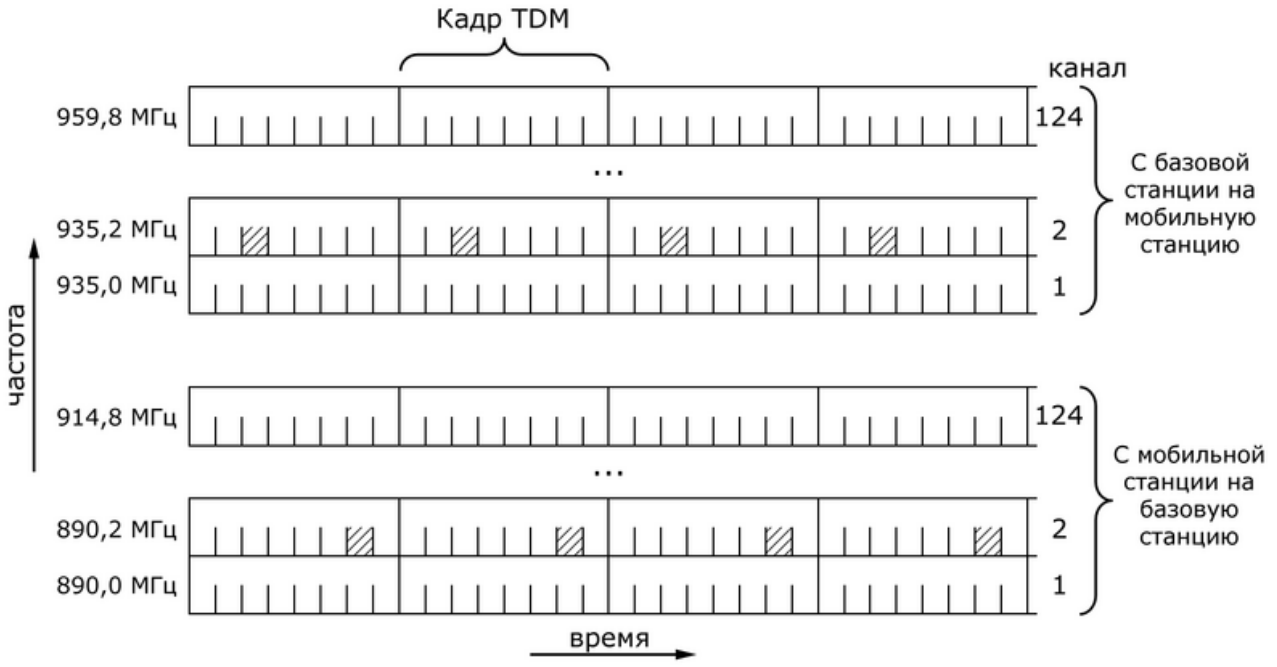


Рис. 21.3. GSM с 124 частотными каналами, в каждом из которых 8-интервальная система с разделением времени

Теоретически каждая сота (ячейка), включающая обслуживаемые одной базовой станцией BTS, может иметь до 992 каналов (124 несущие частоты по 8 временных слотов). Восемь слотов составляют *кадр*.

Однако помехи на одних частотах от мобильных станций смежных сот не позволяет это сделать. Повторное использование частот позволяет существенно повышать ёмкость системы. При этом в близких сотах одна относительно другой используются разные полосы частот, а через несколько сот эти полосы частот повторяются.

На рис. 21.4, а показан принцип повторного использования частот.

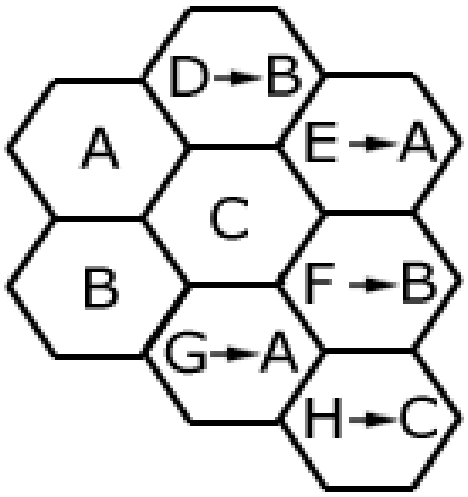


Рис. 21.4, а. Принцип повторного использования частот

Рассмотрим пример. Пусть в некоторой соте (ячейке) используется какая-то часть от полного диапазона частот, например, почти одна десятая. Тогда в соседней с ней ячейке B должна использоваться вторая десятая часть диапазона, поскольку вблизи общей границы в двух смежных ячейках нельзя использовать из-за помех одни и те же частотные каналы. Из тех же соображений в ячейке C придется использовать третью десятую часть диапазона. Но уже в ячейке D, не имеющей границу с ячейкой B, можно вновь использовать ту же десятую часть диапазона, что и в ячейке B. Условно это обозначено DB.

Аналогичные соображения справедливы для ячеек E, F, G, H, так что в итоге мы получаем трехъячеечную схему повторения частот (3-элементный кластер). Такая схема представлена на рис. 21.4 б, где одинаковыми цифрами обозначены ячейки с одинаковыми диапазонами частот. В каждой ячейке при этом используется третья часть всего диапазона частот. При 3-элементном кластере ячейки с одинаковыми полосами повторяются часто, что плохо в смысле уровня взаимных помех от станций, работающих на тех же частотных каналах, но в других ячейках. В этом отношении лучше кластеры с большим числом элементов.

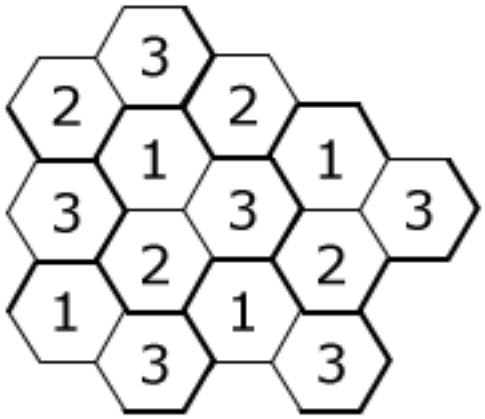


Рис. 21.4, б. 3-элементный кластер

Размер соты GSM может изменяться от нескольких сотен метров до 35 километров в зависимости от окружения (зданий, открытого пространства, гор и т.д.) и ожидаемой интенсивности информационного обмена.

Контроллер базовых станций BSC (Base Station Controller), входящий вместе с BTS в подсистему базовых станций BSS, управляет базовыми станциями BTS. С его помощью происходит резервирование частот и переключение с одной станции BTS на другую, осуществляется поиск мобильных станций. Кроме того, контроллер BSC уплотняет радиоканалы для соединений с проводными каналами через интерфейс A (между подсистемой радиосвязи RSS и подсистемой сетей и коммутации NSS). В основу интерфейса A положены цифровые системы уплотнения каналов E1 с временным уплотнением 30 соединений с пропускной способностью каждого из них 64 Кбит/с.

Мобильная станция включает приемник и передатчик, необходимые для соединения с сетью GSM. В MS входят также модуль идентификации абонента SIM (Subscriber Identity Module), в котором хранятся все индивидуальные данные, необходимые, например, для оплаты аутентификации пользователя. В SIM-карте (выполненной в виде смарт-карты) содержится много идентификаторов и таблиц, например, список абонентских услуг, PIN-код, международный идентификатор мобильного абонента IMSI, данные о местоположении мобильного абонента: TMSI и LAI. Подробное описание структуры мобильной станции приводится в следующем разделе.

21.2.1.2. Подсистема сетей и коммутации

Подсистема сетей и коммутации (NSS) – ядро системы GSM. Она соединяет

беспроводную сеть со стандартными сетями общего пользования ТфОП/ISDN, а также осуществляет переключение подсистем базовых станций BSS. NSS определяет местоположение пользователей в любой точке земного шара, обеспечивает оплату, роуминг пользователей между разными поставщиками услуг связи в разных странах. В состав NSS входят коммутатор и базы данных, состоящие из домашнего регистра HLR и гостевого регистра VLR.

Центр коммутации подвижной (мобильной) связи MSC (Mobile Switching Center) является коммутатором ISDN. MSC устанавливает соединение с контроллерами BSC, другими центрами MSC, образуя стационарную магистральную сеть системы GSM. В большинстве случаев MSC управляет несколькими контроллерами BSC. Шлюз MSC (GMSC) соединен с сетью общего пользования ТфОП/ISDN. Центр MSC управляет всеми сигналами, нужными для установки соединения, разъединения и переключения соединения на другие MSC. В этих целях используется ОКС №7.

Домашний регистр (регистр собственных абонентов) HLR (Home Location Register) представляет собой базу данных мобильных станций, постоянно зарегистрированных в систем конкретного оператора. В HLR хранится вся информация о пользователях. Статическая информация включает номер ISDN мобильного абонента (MSISDN), оплаченные услуги и ключ аутентификации. В HLR содержится динамическая информация, например, данные о текущей зоне местоположения мобильной станции LAI, которые обновляются при переходе MS из текущей зоны. Эти данные нужны, например, для взимания оплаты, для осуществления роуминга.

Гостевой регистр VLR (Visitor Location Register) представляет собой базу данных о мобильных станциях, расположенных в области обслуживания местного центра коммутации MSC. Если в зоне LAI, за которую отвечает регистр VLR , появляется новая мобильная станция, в регистр VLR копируется вся информация об этом пользователе. Такого пользователя или абонента называют роумером и о нем говорят, что он находится в гостевой сети.

21.2.1.3. Операционная подсистема

Третья часть системы GSM – операционная система OSS включает следующее оборудование.

Центр эксплуатации и обслуживания OMC (Operation and Maintenance Center) обеспечивает работу отдельных элементов GSM (MSC, BSC, GMSC и др.). Он выполняет функции администрирования, такие как, тарификация и мониторинг трафика, а также принимает меры в случае отказа отдельных элементов сети. Одна из наиболее важных задач

OMC – это управления телекоммуникациями TMN (Telecommunication Management Network), стандартизированный ITU-T [21]. Слово «network» в названии TMN означает, что для управления элементами сети создается выделенная сеть управления. В больших сетях GSM имеется больше одного OMC и тогда всей сетью управляет центр управления сетью NMC (Network Management Center).

Центр аутентификации AUC(Authentication Centre) представляет базу данных, позволяющую определить – разрешен ли допуск к услугам системы абоненту, имеющему данный модуль идентификации SIM-карту. Центр AUC так же, как SIM-карта абонента содержит секретный ключ абонента, используемый для аутентификации абонента и шифрования на радиоучастке. AUC содержит значения, необходимые для аутентификации, алгоритмы аутентификации и шифрования и др.

Регистр идентификации оборудования EIR (Equipment Identity Register) представляет базу данных, содержащую список всего разрешенного в сети оборудования.

Каждая мобильная станция может быть идентифицирована её кодом IMEI, который помечает запрет в определенных случаях (устройство украдено, не поддерживается сетью и др.)

21.2.2. Логические каналы и установление связи

Все физические каналы (слоты) используются для выполнения различных функций. Деление каналов по выполняемым ими конкретным функциям производится с помощью понятия логического канала, которые составляют две группы - каналы информационного обмена и каналы управления.

Каналы информационного обмена TCH (Traffic Channel) используется для передачи пользовательских данных (речь, данные).

Каналы управления делятся на три типа:

- Широковещательный управляющий канал (BCCH) используется для передачи непрерывного потока от базовой станции ко всем мобильным в вещательном режиме (подстройка частоты, мониторинг мощности сигнала для определения момента перехода MS в обслуживание другой соты и др.);
- Общий канал управления (CCCH) предназначен для вызова MS базовой станцией, для назначения закрепленного канала управления (передается также с базовой станции);
- Выделенный закрепленный канал управления (SDCCH) используется для поиска MS, обновления информации о нем, регистрации и установления соединения.

Каждая из перечисленных групп разделяется на подгруппы типов каналов. На рис. 21.5 представлена упрощенная схема установления исходящего вызова.

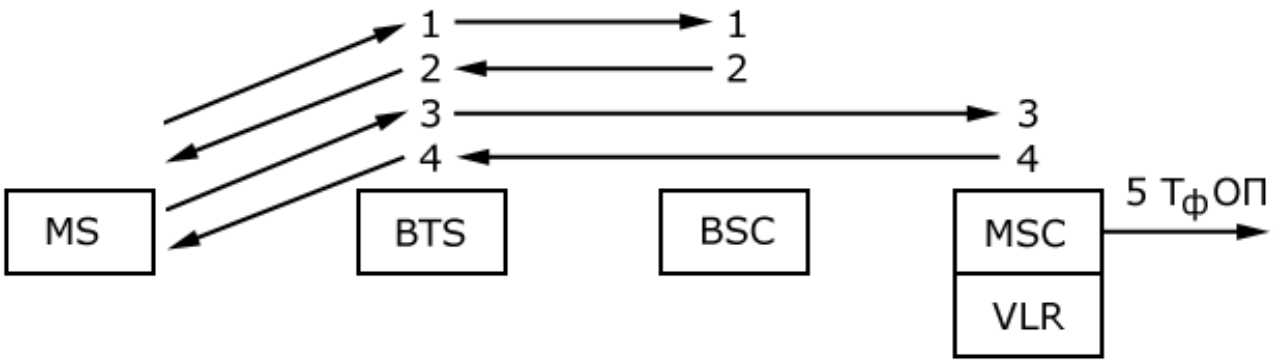


Рис. 21.5. Упрощенная схема установления исходящего вызова

Цифрами обозначена следующая последовательность действий.

- Мобильная станция MS через один их типов каналов (канал случайного доступа RACH) группы общих каналов управления CCCH запрашивает выделенный закреплённый канал управления (SDCCH) группы выделенных каналов управления DCCH для установления связи.
- Контроллер базовой станции BSC через канал разрешения (AGCH) группы общих каналов управления CCCH назначает канал SDCCH.
- Мобильная станция MS через канал SDCCH проводит аутентификацию и выдает запрос на вызов (с номером вызываемого абонента).
- Центр коммутации MSC выдает команду назначение канала трафика THC.
- Центр коммутации MSC передает вызываемый номер на ТФОП/ISDN, а после ответа вызываемого абонента завершает соединение.

Процедура установления связи практически не отличается, если мобильная станция вызывает мобильную станцию.

В каждом временном слоте передается информационный пакет из 148 битов. 26 информационных кадров объединяются в мультикадры. Мультикадр канала управления состоит из 51 кадра канала управления. Мультикадры в свою очередь, объединяются в суперкадры: дин суперкадр состоит из 51 мультикадра информационных кадров или 26 мультикадров канала управления. Длительность суперкадра в обоих случаях составляет 1326 кадров.2048 суперкадров образуют один гиперкадр с 2715648 кадрами. Кадры пронумерованы от 0 до 2715648. Номер кадра используется в процессе шифрования передаваемой информации.

21.3. Обработка речевых сигналов на радиоучастке

Описание обработки речевого сигнала на радиоучастке приводится на упрощенной схеме приемо-передатчика мобильной станции (рис. 21.6).

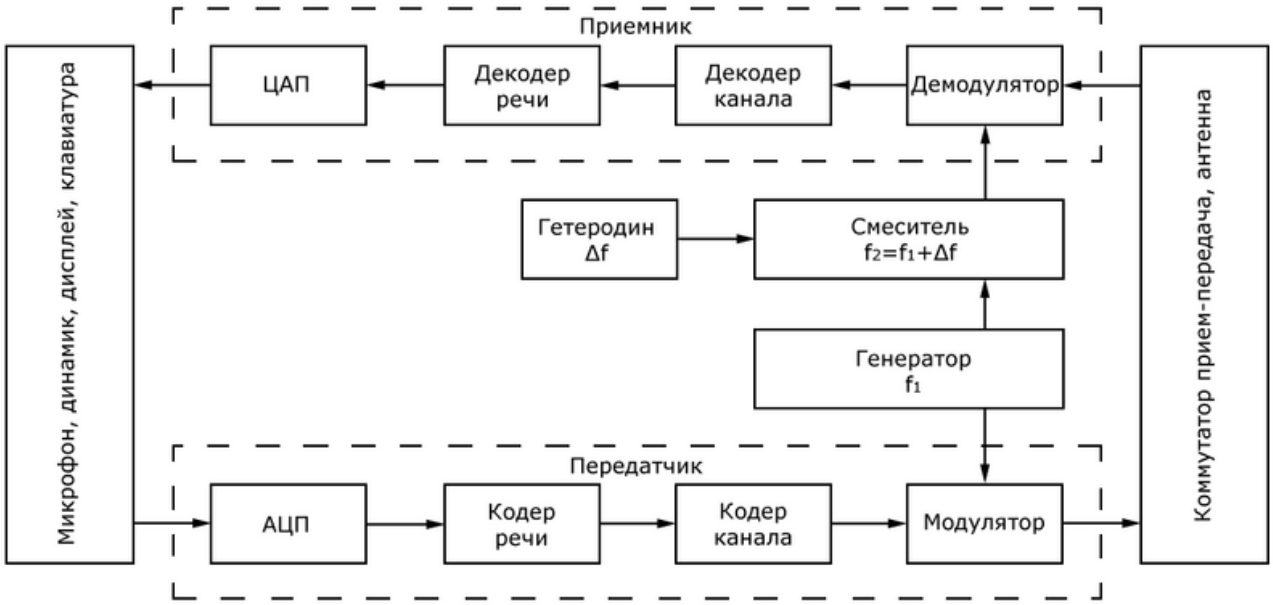


Рис. 21.6. Упрощенная блок-схема приемо-передатчика мобильной станции

Так как аналогичные блоки содержатся и в базовой станции, поэтому ограничимся описанием только мобильной станцией.

В микрофоне речевой сигнал преобразуется в электрический, ширина спектра которого ограничена фильтром и составляет 4 КГц. В состав передатчика и приемника входят следующие блоки.

- Аналого-цифровой преобразователь (АЦП) преобразует в цифровую форму сигнал с выхода микрофона. Последующая обработка и передача сигнала речи производится в цифровой форме, вплоть до обратного цифро-аналогового преобразования (ЦАП) на приеме.
- Кодер речи осуществляет кодирование сигнала речи в цифровой форме с целью сокращения объема информации, передаваемой по каналу связи. Декодер речи восстанавливает на приеме поступивший на него закодированный сигнал речи.
- Кодер канала добавляет в сигнал закодированной речи дополнительную информацию, предназначенную для защиты от ошибок на радиоучастке. Декодер канала проверяет

принятую информацию на наличие ошибок и выявленные ошибки по возможности исправляет.

- Модулятор осуществляет перенос информации на несущую частоту. Демодулятор выделяет из модулированного радиосигнала несущую информацию.

Рассмотрим все этапы обработки.

21.3.1. Кодер речи

Кодер речи является первым элементом цифрового участка передающего тракта, следующим после АЦП. На вход кодера речи поступает поток информации со скоростью 64 *Кбит/с*. Основная задача кодера (encoder) речи – уменьшение скорости передачи, т.е. предельно возможное сжатие сигнала речи, но при сохранении приемлемого качества передачи речи. В приемном тракте перед АЦП размещен декодер речи. Задача декодера (decoder) – восстановление обычного цифрового сигнала речи. В GSM используется кодирование речи на основе линейного предсказания LPC (Liner Predictive Coding). Суть этого метода заключается в том, что по каналу связи передаются не параметры речевого сигнала, а параметры некоторого фильтра, эквивалентного голосовому сигналу, и параметры возбуждения этого фильтра. Задача кодирования на передающем конце канала связи заключается в оценке параметров фильтра и параметров сигналов возбуждения, а задача декодирования на приемном конце – в пропускании сигнала возбуждения через фильтр, на выходе которого получается восстановленный сигнал речи. Метод линейного предсказания заключается в том, что очередная выборка речевого сигнала с некоторой степенью точности предсказывается линейной комбинацией m предшествующих выборок. Для каждого 20-миллисекундного сегмента оцениваются параметры фильтра кратковременного линейного предсказания, составляющие 260 бит информации. Таким образом, кодер речи осуществляет сжатие информации в 4.92 раза – (64 *Кбит/с**20 *мс*)/260 *бит*, а скорость потока данных на выходе речевого кодера уменьшается с 64 *Кбит/с* до 13*Кбит/с*.

При оценке качества кодирования и сопоставлении кодеров оцениваются разборчивость речи и качество синтеза (качество звучания) речи. Для оценки разборчивости речи используют метод DRT (Diagnostic Rhyme Test – диагностический рифмованный тест). В этом методе подбираются пары близких по звучанию слов, отличающихся отдельными согласными (типа «дот – кот», «кол – гол»), которые многократно произносятся рядом дикторов, и по результатам испытаний оценивается доля искажений. Метод позволяет получить как оценку разборчивости отдельных согласных, так и общую оценку

разборчивости речи.

Для оценки качества звучания используется критерий DAM (Diagnostic Acceptability Measure – диагностическая мера приемлемости). Испытания заключаются в чтении несколькими дикторами мужчинами и женщинами, ряда специально подобранных фраз, которые прослушиваются на выходе тракта связи рядом экспертов-слушателей, выставляющих свои оценки по пятибалльной шкале. Результатом является средняя субъективная оценка, или средняя оценка мнений (Mean Opinion Score – MOS). Хотя этот метод является субъективным по своей сути, его результаты по сопоставлению различных типов кодеков при проведении испытаний одними и теми же группами дикторов и экспертов- слушателей являются достаточно объективными. В качестве примера в табл. 21.3 приведены результаты оценки используемого в GSM кодека по сравнению с импульсно-кодовой модуляцией без использования сжатия методом линейного предсказания.

Таблица 21.3. Оценка кодеков речи по шкале MOS

Тип кодека	Скорость передачи информации, Кбит/с	Оценка MOS
ИКМ	64	4.12
RPE-LTP (стандарт GSM)	13	3.58

21.3.2. Кодер канала

Основная задача кодека канала – помехоустойчивое кодирование/декодирование сигнала речи, т.е. такое кодирование которое позволяет обнаружить и в значительной мере исправить ошибки, возникающие на радиоучастке, т.е. между BTS и MS. Методы обнаружения ошибок применяются в протоколах управления каналами передачи данных, таких как HDLC, а также транспортных протоколах, таких как TCP. При этом имеется в виду повторная передача искаженных в канале блоков данных. Для беспроводных каналов характерен высокий уровень ошибок, в результате чего потребуется недопустимо большое число повторных передач, что для речевых сообщений недопустимо из-за больших задержек. Используемые в сотовой связи дециметровые волны, распространяются в основном по прямой, но испытывают многочисленные отражения от крупных объектов. При сложении нескольких сигналов, прошедших по разным путям и имеющих в точке приема в общем случае различные фазы, результирующий сигнал может быть как выше среднего уровня, так и заметно ниже. Образующиеся *замирания сигнала* (колебания уровня) бывают достаточно глубокими, и при этом отношение сигнал/шум падает настолько сильно, что полезная информация может существенно искажаться шумами, вплоть до полной ее потери. В сети GSM для борьбы с замиранием, а также с межсимвольной интерференцией может использоваться расширение спектра методом перескока частоты или скачков по частоте (frequency hopping). Метод скачков по частоте состоит в том, что несущая частота для каждого физического канала периодически переводится на новый частотный канал. При изменении частоты замирание с большей вероятностью не будет. Следовательно, при достаточно частых изменениях частоты существенно снижается вероятность длительных замираний и соответственно снижается вероятность групповых ошибок. С одиночными ошибками можно успешно бороться с помощью помехоустойчивого кодирования, о чем подробно будет изложено в настоящем разделе.

По качеству речи, воспроизводимой с помощью кодека речи GSM, биты в 260-битовом блоке можно разделить на три класса:

- Класс 1a: 50 бит, наиболее чувствительные к битовым ошибкам.
- Класс 1b: 132 бита, умеренно чувствительные к битовым ошибкам.
- Класс 2a: 78 бит, минимально чувствительные к битовым ошибкам.

Для защиты первых 50 бит используется 3-битовая проверка с помощью циклического кода. При обнаружении ошибки – весь блок 260 бит отбрасывается и заменяется предыдущим. Эти

53 бита при необнаруженной ошибке, 132 бита класса 1b, а также 4 - битовая остаточная последовательность нулей (т.е. всего 189 бит), затем защищаются сверточным кодом. Сверточный код используется для исправления одиночных ошибок. Коды с исправлением ошибок называются прямой коррекцией ошибок FEC (Forward Error Correction).

При сверточном кодировании (рис. 21.7) K последовательных символов входной информационной последовательности, по k бит в каждом символе участвуют в образовании n-битовых символов выходной последовательности, n > k, причем на каждый символ входной последовательности приходится по одному символу выходной.

Каждый бит выходной последовательности получается в результате суммирования по модулю 2 нескольких бит (от двух до Kk бит) K входных символов, для чего используются n сумматоров по модулю 2. Сверточный кодер с параметрами n, k, K обозначается (n, k, K).

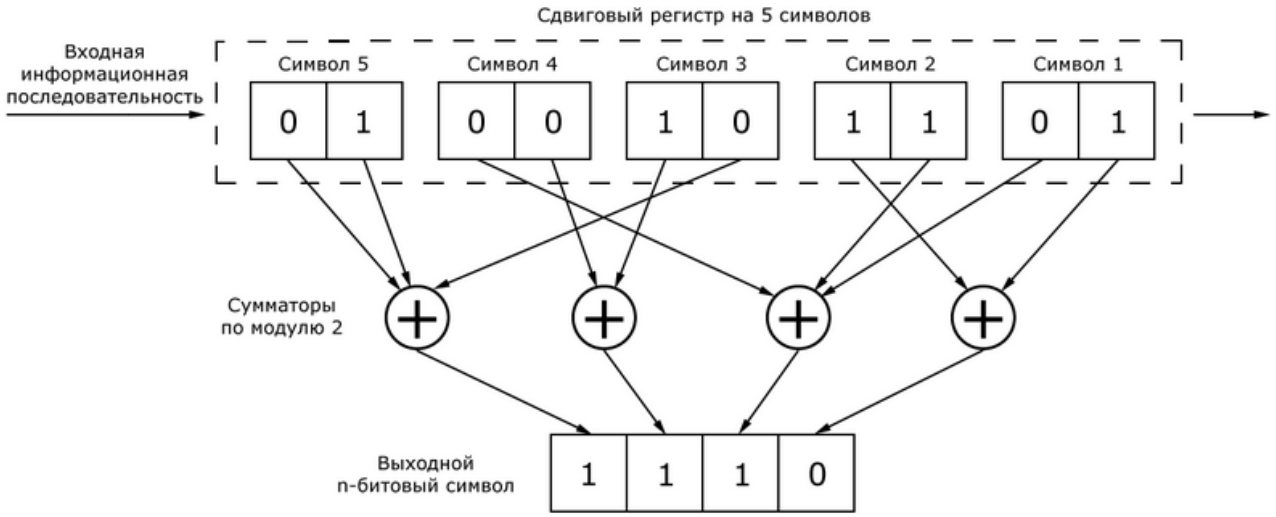


Рис. 21.7. Схема сверточного кодера *(4, 2, 5)*
(n = 4, k =2; R = k/n = ½)

Отношение R=k/n называется *скоростью кодирования кодера*. Параметр K называется длиной ограничения и определяет длину сдвигового регистра (в символах), содержимое которого участвует в формировании одного выходного символа.

После того как очередной выходной символ сформирован, входная последовательность сдвигается на один символ вправо, в результате чего символ 1 выходит за пределы регистра, символы 2, 3, 4, 5 перемещаются вправо, каждый на место соседнего, а на освободившееся место записывается очередной символ входной последовательности, и по новому содержимому регистра формируется следующий выходной символ. Если k = 1, т.е. символы

входной последовательности однобитовые, сверточный кодер называется двоичным. Сверточный кодер, схема которого приведена на рис. 21.7 не является двоичным, поскольку для него k = 2.

В случае GSM 189 бит речевого сигнала защищаются сверточным кодом (2, 1, 5), что в итоге составляет 456 бит (189*2 плюс 78 бит незащищенные). В результате на выходе кодера канала скорость потока данных увеличивается с 13 *Кбит/с* до 22.8 *Кбит/с* - (13 *Кбит/с**456*бит*/260*бит).*

На рис. 21.8 приведено описанное выше канальное кодирование 20-миллисекундного сегмента речи.

Рис. 21.8. Канальное кодирование 20-миллисекундного сегмента речи

Сверточный код (2.1.5) используется для исправления одиночных ошибок. Кодированный блок сегмента речи подвергается перемежению. Примем в качестве меры избыточности, вносимую кодированием, отношение длины исходной информации к длине информации, передаваемой в канал. Будем называть это значение скоростью кодирования. В данном случае для сегмента речи эта величина равна 260/456, т.е. 0,57. Высокая избыточность кодирования при исправлении одиночной ошибки не позволяет использовать кодирование с большей исправляющей способностью (т.е. двойные и более ошибки). Перед выдачей в канал связи закодированная информация речи также подвергается перемежению. Перемежение представляет собой такое изменение порядка следования символов информационной последовательности, т.е. такую перестановку, или перетасовку, символов, при которой стоявшие рядом символы оказываются разделенными несколькими другими символами.

Такая процедура предпринимается с целью преобразования групповых ошибок (пакетов ошибок) в одиночные с которыми легче бороться с помощью кодирования. Использование перемежения – одна из характерных особенностей сотовой связи, и это является следствием неизбежных глубоких замираний сигнала в условиях многолучевого распространения, которое практически всегда имеет место, особенно в условиях плотной городской застройки. При этом группа следующих один за другим символов, попадающих на интервал замирания (провала) сигнала, с большой вероятностью оказывается ошибочной. Если же перед выдачей информационной последовательности в радиоканал она подвергается процедуре перемежения, а на приемном конце восстанавливается прежний порядок следования символов, то пакеты ошибок с большой вероятностью рассыпаются на одиночные ошибки. Известно несколько различных схем перемежения и их модификаций – диагональная, блочная, сверточная и другие. Мы кратко рассмотрим первые две из них, лежащие в основе схем, применяемых в сотовой связи.

При диагональном перемежении входная информация делится на блоки, а блоки – на субблоки, и в выходной последовательности субблоки, например, второй половины предыдущего блока чередуются с субблоками первой половины следующего блока. Такая схема иллюстрируется на рис. 21.9, где каждый блок состоит из шести субблоков, и субблоки первого блока обозначены a_i, второго – b_i, третьего – c_i. Субблок может состоять из нескольких символов, или из одного символа, или даже из одного бита. Приведенная схема диагонального перемежения вносит малую задержку, но расставляет соседние символы лишь через один, т.е. рассредоточение ошибочных символов группы получается сравнительно небольшим.

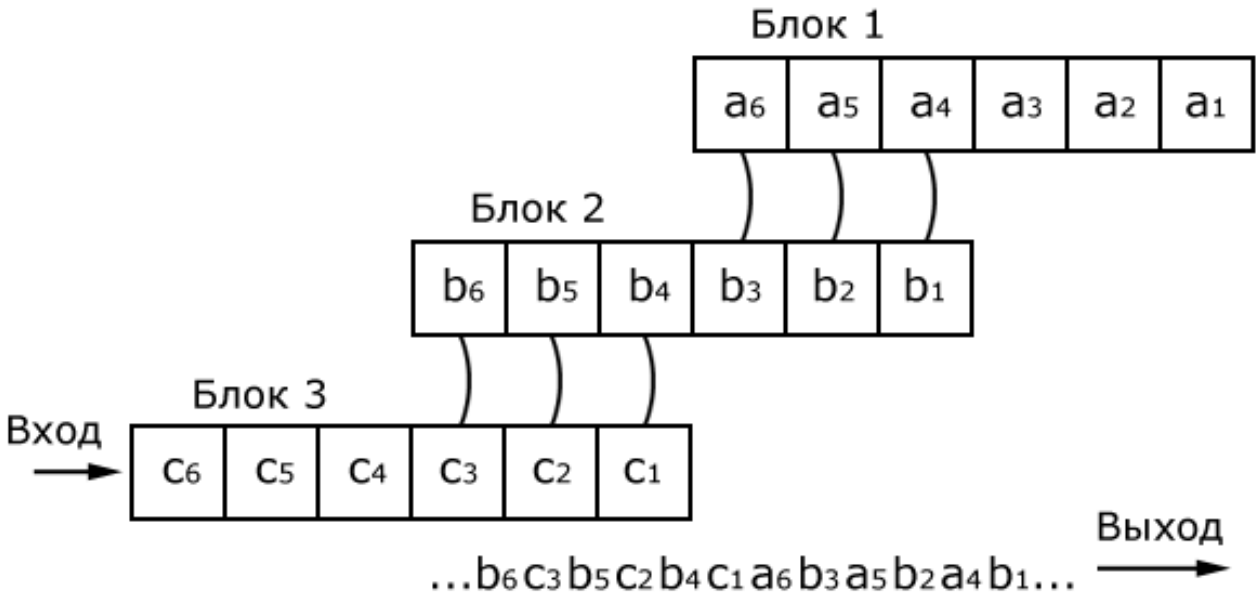


Рис. 21.9. Пример схемы диагонального перемежения

При блочном перемежении входная информация также делится на блоки по n субблоков (или символов) в каждом, и в выходной последовательности чередуются субблоки k последовательных блоков. Работу этой схемы можно представить себе в виде записи блоков входной последовательности в качестве строк матрицы размерности k*n (рис. 21.10), считывание информации из которой производится по столбцам. Следовательно, если входная последовательность в этом примере имела вид $a_1,a_2,...,a_n,b_1,b_2,...,b_n,k_1,k_2,...,k_n$, то выходная будет такой: $a_1,b_1,...,k_1,a_2,b_2,...,k_2,a_n,b_n,...,k_n$. Субблоки, или символы, в частном случае здесь также могут состоять лишь из одного бита. Схема блочного перемежения вносит большую задержку, чем диагонального, но значительно сильнее рассредоточивает символы группы ошибок.

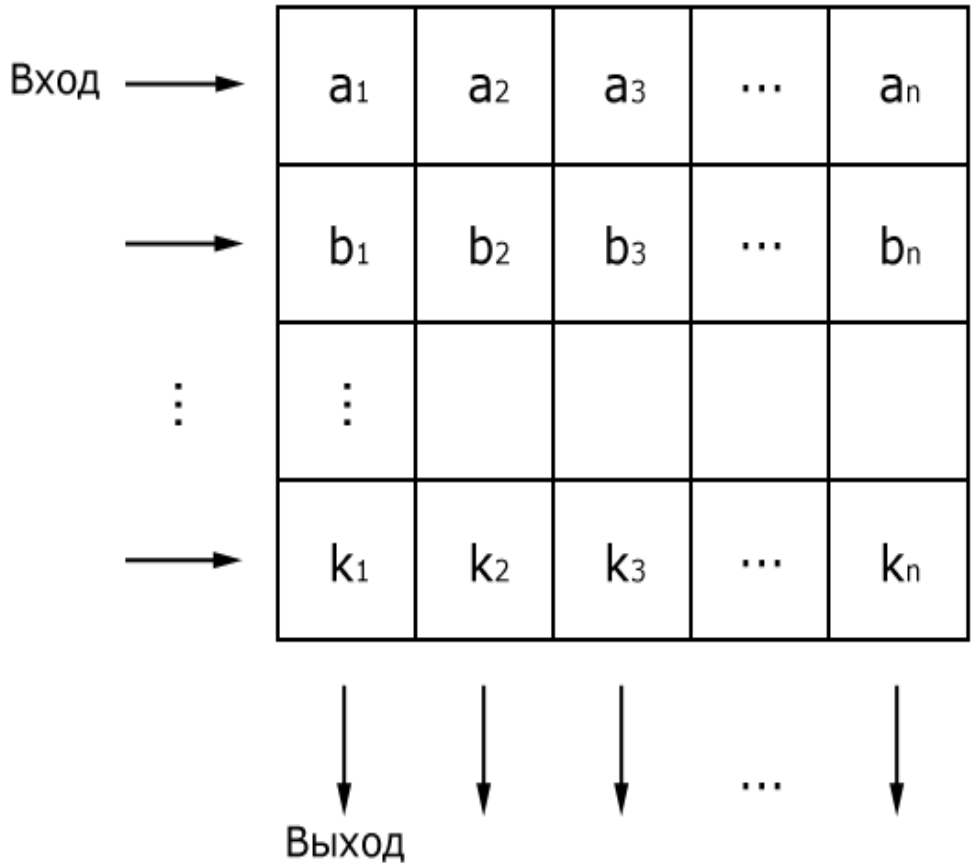


Рис. 21.10. Схема блочного перемежения

В стандарте GSM используется достаточно сложная и совершенная схема блочно-диагонального перемежения. 456 бит информации одного 20-миллисекундного сегмента речи разбиваются на 8 подсегментов. 57 бит одного подсегмента распределяются между смежными восемью подсегментами таким образом, что после перемежения смежными с каждым конкретным битом оказываются соответствующие ему по положению биты, отстоявшие от него до перестановки на 4 подсегмента, причем на четные и нечетные (после перестановки) битовые позиции подсегмента ставятся биты из смежных сегментов. Алгоритм перемежения обладает свойствами квазислучайности, так что смежные биты исходной последовательности оказываются разделенными непостоянным числом бит, что является преимуществом в борьбе с периодическим битовыми ошибками. Вносимая задержка речи составляет существенную величину порядка 70-80 мс и включает порядка 20 мс на кодек речи, 10-20 мс на кодек канала и 40 мс на перемежение и деперемежение.

Информация каналов управления подвергается блочному и сверточному кодированию в

полном объеме. Так, для кодирования информации каналов SACCH, FACCH, FCCH, PCH, AGCH, SDCCH используется блочный кодер (224, 184), сверточный кодер (2, 1, 5) и та же схема перемежения, что и для канала трафика. В каналах RACH, SCH используются другие схемы блочного кодирования, а также сверточные кодеры (2, 1, 5), отличающиеся от сверточных кодеров перечисленных ранее каналов управления. При передачи данных используются более сложные схемы сверточного кодирования и перемежения, обеспечивающие соответственно и более высокое качество передачи информации. На рис. 21.11 приведена схема кодирования блока сигналов управления между мобильной станцией MS и базовой станцией BTS. При передачи управляющих сообщений используется кодирование с более сильной коррекцией ошибок, чем при передаче речи. Управляющее сообщение состоит из 23 байт, т.е. 184 бит. При кодировании к управляющему сообщению (блоку данных) добавляется 40 бит контрольно-проверочной комбинации блочного циклического кода CRC.

Скорость кодирования блоков символов управления равна 184/456=0,4. Это значит, что избыточность кодирования выше, чем в случае сегмента речи, схема которого приведена выше на рис. 21.10.

Рис. 21.11. Канальное кодирование блока символов управления

21.3.3. Модуляция

Модулятор является последним элементом передающего тракта (рис. 20.8) и, строго говоря, не выполняет никаких операций собственно цифровой обработки сигналов. Его задача состоит в переносе информации цифрового сигнала с выхода кодера канала на несущую частоту, т.е. в модуляции сверхвысокочастотной (СВЧ) несущей низкочастотным (НЧ) цифровым сигналом. Модулированный СВЧ сигнал с выхода модулятора через антенный коммутатор поступает на антенну и излучается в эфир, чтобы быть затем принятым антенной станции-получателя информации. Соответственно демодулятор – первый элемент приемного тракта, и его задача заключается в выделении из принятого модулированного радиосигнала информационного сигнала, который подвергается цифровой обработке в последующей части приемного тракта.

Как известно, существуют три основных вида модуляции: это амплитудная модуляция – АМ (Amplitude Modulation – AM), частотная модуляция – ЧМ (Frequency Modulation – FM) и фазовая модуляция – ФМ (Phase Modulation – PM). Между тем, в цифровой сотовой связи фигурируют такие названия, как квадратурная фазовая модуляция (Quadrature Phase Shift Keying – QPSK), бинарная фазовая модуляция (Binary Phase Shift Keying) и др. На самом деле, это не что иное, как разновидности фазовой или частотной модуляции, предназначенные для передачи дискретных (цифровых) сигналов. В стандарте GSM используется гауссовская модуляция MSC с минимальным сдвигом (*Gaussian Minimum Shift Keying* – GMSK). В основу схемы MSK положена двоичная частотная манипуляция без резких изменений фазы, т.е. MSK относится к схемам модуляции без разрыва фазы. Напомним о комбинированной амплитудной модуляции QAM (глава 3, раздел 3.4), широко используемой в беспроводных сетях связи GSM, WiMAX и др.

21.4. Информационная безопасность GSM

На радиоучастке GSM реализованы следующие механизмы информационной безопасности - шифрование/дешифрование речи между мобильной станцией и базовой станцией, а также аутентификация мобильной станции. Кроме этого предусмотрена защита местоположения мобильной станции, которое рассматривается приватными данными [71].

21.4.1. Конфиденциальность

Алгоритм шифрования (A5) реализуется в мобильной станции. Активация этого алгоритма инициируется сетью (рис. 21.12). Как видно из рисунка данные информационного и управляющего канала на радиоучастке передаются в зашифрованном виде. В процессе

шифрования используется стандартизированный ETSI алгоритм поточного шифрования (см. Приложение Б) A5, который реализуется в MS и в оборудовании операционной подсистемы GSM - центре аутентификации AUC. В SIM-карте на основании индивидуального секретного ключа K_i и случайного числа RAND, полученного из сети, формируется ключ шифрования Kc. Этот ключ вычисляется по алгоритму (A8), который хранится в SIM-карте.

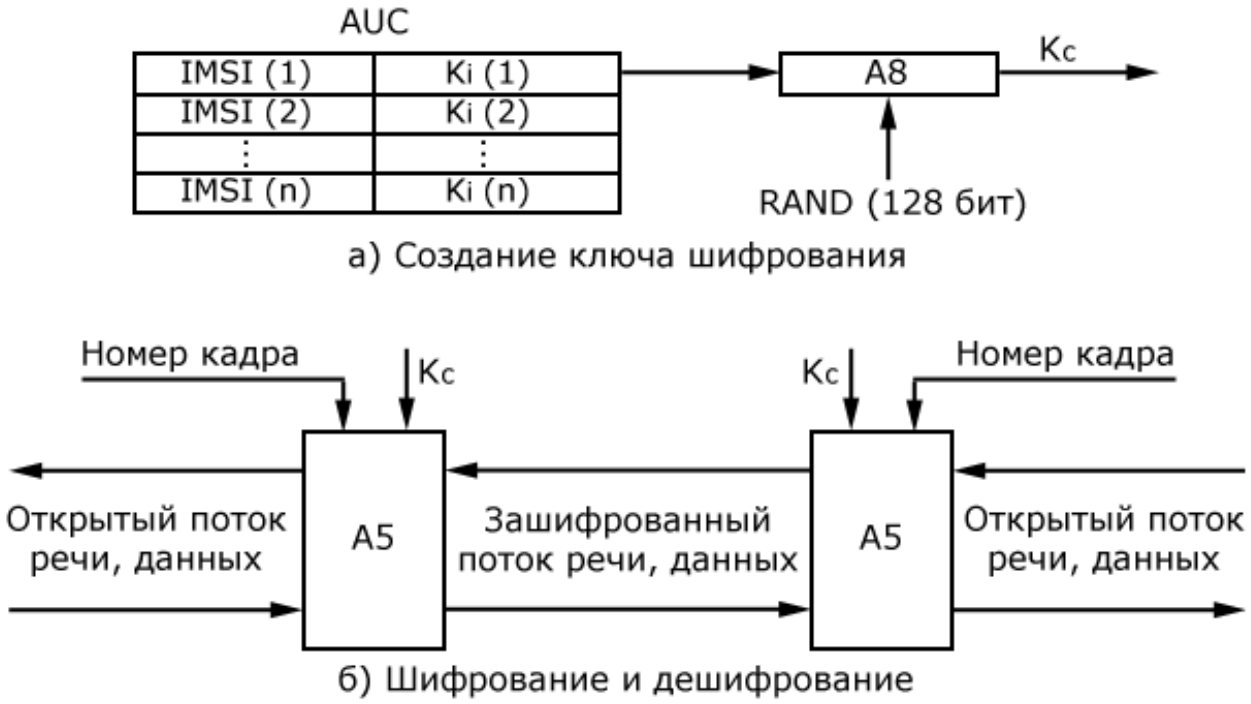


Рис. 21.12. Шифрование/дешифрование потока речи, данных

Логические каналы не могут использовать временные интервалы (слоты) произвольным образом. Восемь слотов составляют кадр. В системе GSM применяется довольно сложная схема уплотнения, объединяющая несколько иерархий кадров. В каналах трафика и ассоциированных с ними каналах управления 26 кадров образуют *мультикадр*. В свою очередь 51 мультикадр составляет *суперкадр*. 2048 суперкадров образуют высший уровень временной иерархии системы GSM – *гиперкадр*. Гиперкадр имеет продолжительность почти 3.5 часа и включает 2715648 временных слотов. Такая логическая структура нужна для процедуры шифрования на радиоучастке – номера кадра используют для увеличения уровня конфиденциальности разговора.

На основе полученного ключа K_C и текущего 22-битового номера кадра по алгоритму A5 формируется псевдослучайная последовательность и производится поточное шифрование/дешифрование кадра на радиоучастке. Процедура создания нумерованных

кадров в пределах гиперкадра приведена выше в настоящей главе (раздел 21.2.2). Использование текущего 22-битового номера кадра позволяет повысить уровень безопасности шифрования. В фиксированной части сети та же операция выполняется в отношении принимаемого блока из 114 зашифрованных битов. Если при передаче данных по радиоканалу не возникло ошибок, то прибавление по модулю 2 сгенерированной шифрующей последовательности к принятому блоку данных приводит к восстановлению первоначальной информационной последовательности, сгенерированной в мобильной станции. Таким образом, реализуется дешифрование.

21.4.2. Аутентификация пользователя

Алгоритм аутентификации пользователя мобильной станции GSM основан на протоколе ОКЛИК-ОТЗЫВ (см. приложение Г) и является вторым этапом аутентификации. Первый этап аутентификации пользователя в GSM основан на однопроходном методе с использованием PIN-кода и во многом похож на приведенный механизм аутентификации пользователя ISDN (глава 17).

В сети GSM аутентификация пользователя (рис. 21.13) производится путем проверки подлинности SIM-карты (Subscriber Identity Module – модуль идентификации абонента), расположенной в мобильной станции. В SIM-карте и в центре аутентификации AUC хранятся:

- ключ K_i пользователя i;
- алгоритм расчета отзыва A3.

По алгоритму A3 (рис. 21.13, а) производится вычисление отзыва SRES (Signed Response) на основании:

- оклика RAND длиной 128 бит;
- ключа K_i пользователя i. В AUC ключ каждого пользователя связан с международным идентификатором IMSI этого пользователя.

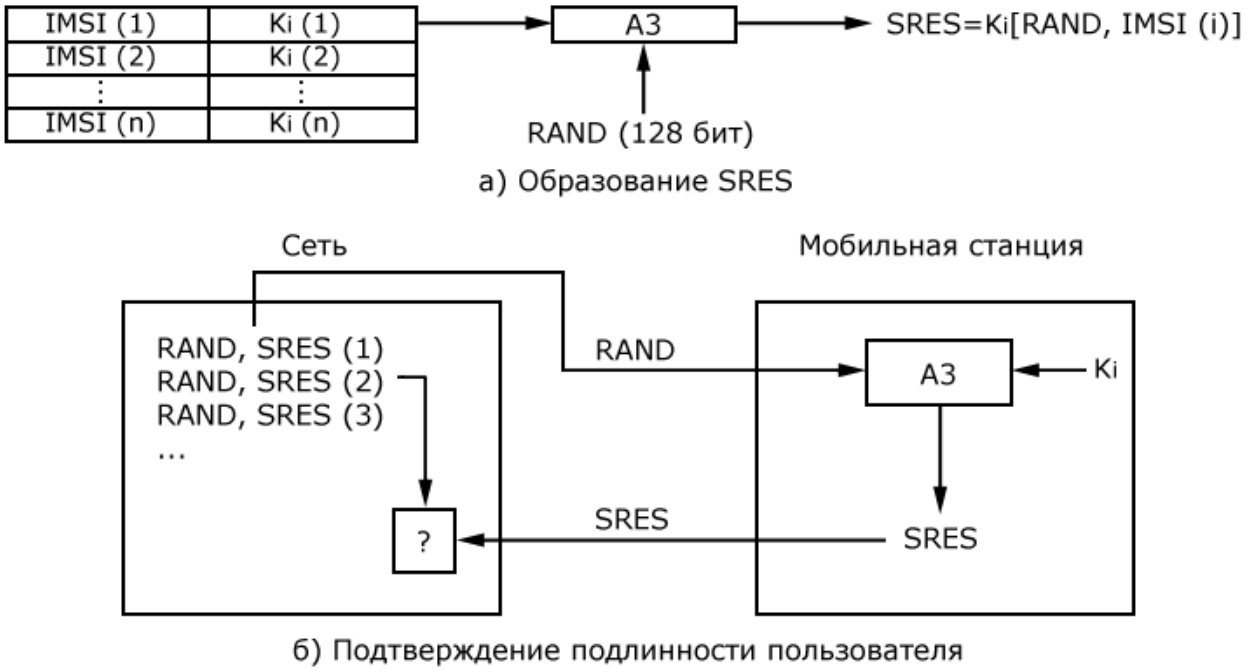


Рис. 21.13. Аутентификация пользователя в GSM

В целях аутентификации пользователя сеть посылает пользователю оклик RAND в сообщении (рис. 21.13, б). Мобильная станция вычисляет отзыв SRES и возвращает его в сеть. Если величина SRES равна заранее вычисленной в сети, аутентификация пользователя завершается успешно.

21.4.3. Защита приватных данных

Каждому абоненту назначается уникальный номер, который известен как международный индентификатор мобильного абонента IMSI. Он представляет собой уникальный идентификатор абонента в сети сотовой связи GSM и записан в SIM-карте. IMSI состоит из кода страны постоянного места жительства, кода сети GSM-оператора (т.е. кода регистра HLR) и идентификационного номера мобильной станции. Использование при аутентификации пользователя его международного идентификатора IMSI накладывает требование на его скрытие для защиты от незаконного получения приватных данных, к которым относится местоположение мобильной станции. Перехват IMSI на радиоучастке позволяет нарушителю обнаружить личность пользователя, передающего сообщение. С целью защиты от этой угрозы ИБ значение IMSI передается только один раз при первом соединении мобильной станции с сетью. Производится это по запросу от сети, к которой

приписана мобильная станция. В этот момент сеть не знает IMSI. Для того чтобы можно было вызывать мобильную станцию или для возможности мобильной станции установить соединение, необходимо выполнить **процедуру регистрации**. В SIM-карте мобильной станции содержится идентификатор области местоположения мобильного абонента LAI (Local Area Identity). Регистрация производится, если LAI, переданный на мобильную станцию MS с базовой станции, отличается от хранимого в памяти SIM-карты. Обновление информации о местоположении LAI производится периодически, что позволяет отслеживать перемещение MS и ее текущее состояние.

Процедура регистрации (обновления местоположения MS) начинается после включения питания мобильной станции. При этом MS посылает на базовую станцию запрос на проведение регистрации. Запрос содержит идентификатор области местоположения MS (LAI) и временной идентификатор мобильной станции TMSI (Temporary Mobile Subscriber Identity), значение которого уникально для каждой станции. Запрос попадает в MSC и в VLR через базовую станцию и контролер базовой станции. Если VLR уже содержит тот же TMSI мобильной станции, то обновляется информация только об активизации мобильной станции.

Использование TMSI вместо IMSI позволяет исключить возможность злоумышленнику определить местоположение абонента. TMSI необходимо для выполнения процедуры аутентификации пользователя в GSM, т.е. для формирования в сети отзыва SRES, соответствующего именно этому пользователю (рис. 21.13, а).

Рассмотрим случай, когда в VLR нет TMSI пользователя, запрашивающего регистрацию. В этом случае производится декодирование LAI, полученного от мобильной станции. LAI косвенно определяет VLR, который ранее обслуживал данную MS. После установления соединения текущего VLR с предыдущим, последний передает параметры пользователя текущему VLR, в том числе TMSI.

Процедура аутентификации пользователя, описанная выше, выполняется после завершения процедуры регистрации с помощью анализа TMSI. После завершения аутентификации пользователя устанавливаются новые параметры мобильной станции TMSI и LAI. Эта информация обновляется в VLR и HLR. Строго говоря, HLR инициирует удаление информации о пользователе из предыдущего VLR и перенос ее в новый VLR. Новые параметры TMSI и LAI передаются мобильной станции из VLR, причем TMSI должен передаваться по радиоканалу в зашифрованном виде.

ГЛАВА 22. Система ОКС№7 в GSM. Информационная безопасность ОКС№7 в ССОП

22.1. Архитектура протоколов передачи сигналов в GSM

На рис. 22.1 приведена упрощенная диаграмма протоколов и используемых интерфейсов передачи сигналов между мобильной станцией MS, базовой станцией BTS, контроллером базовой станции BSC и мобильной станцией MSC.

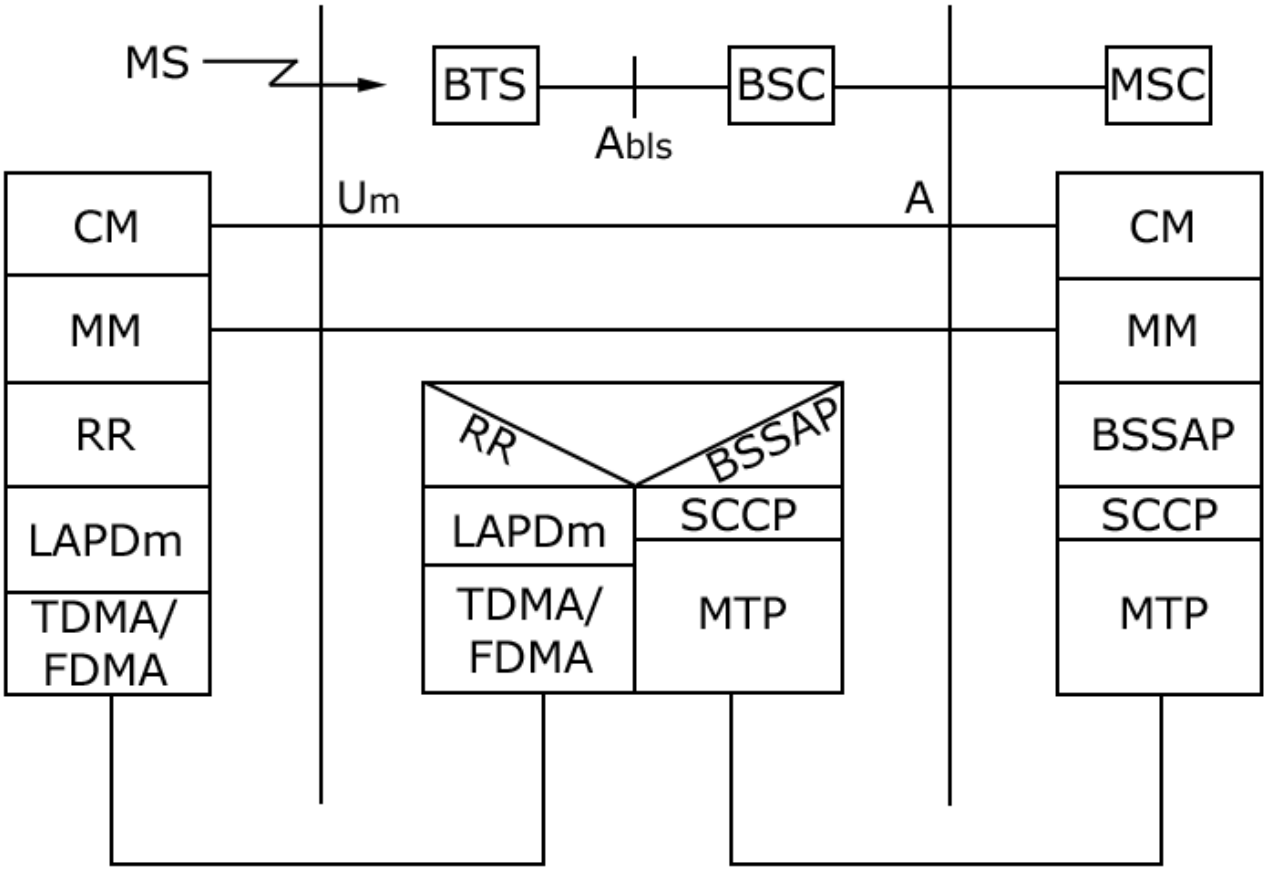


Рис. 22.1. Диаграмма протоколов передачи сигналов в GSM

Физический уровень выполняет функции временного уплотнения восьми слотов в кадр определенной полосы частот, выбор свободных каналов, кодирование (декодирование) речи, кодирование (декодирование) канала, модуляцию (демодуляцию). На диаграмме этот уровень обозначен TDMA/FDMA. На втором уровне используется протокол канального уровня LAPD (тот же самый, который используется на абонентском доступе ISDN). На участке MS-BTS этот протокол модифицирован LAPDm, так как функции обнаружения и исправления ошибок выполняются в GSM на физическом уровне при кодировании/декодировании канала. Уровень

RR (Radio Resourse) используется для установления, обслуживания и освобождения радиоканала.

Уровень управления мобильностью MM (Mobility Management) выполняет функции по обеспечению сетевой безопасности (регистрация, аутентификация, обновление информации о местонахождении пользователя).

Уровень CM (Call Management) функционально разделен на три объекта - управление вызовами (CC), служба коротких сообщений (SMS) и дополнительные службы (SS). Для передачи SMS используются каналы управления, что и позволяет получать сообщения во время передачи речи.

Процедуры CC используются для установления и разъединения соединений, а также для изменения его параметров.

Дополнительные службы –SS (Supplementary Service), могут быть разные (переадресация, замкнутая группа абонентов, идентификация пользователя и др.).

Различные функциональные элементы GSM (например, регистры HLR, VLR, центры коммутации MSC и т.п.) используют различные протоколы ОКС№7. На рис. 22.2 приведены протоколы ОКС№7 для участка сети, состоящего из коммутатора GSM MSC и коммутатора ТфОП/ISDN.

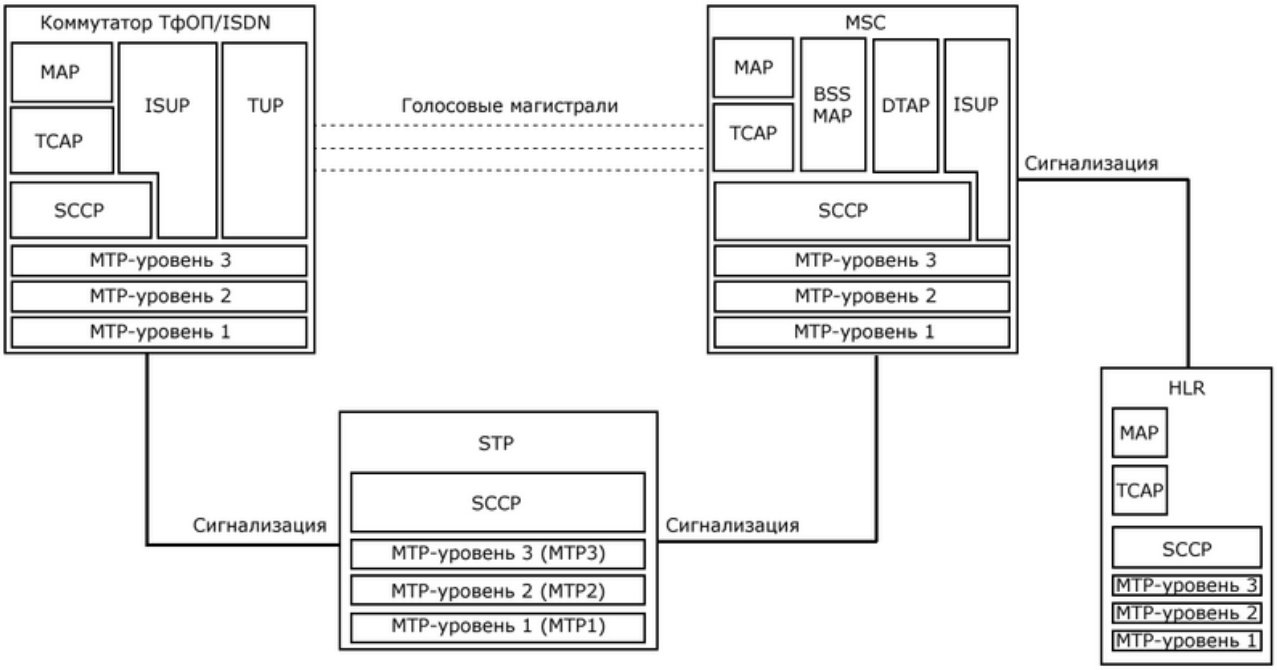


Рис. 22.2. Протоколы ОКС№7 участка MSC-коммутатор ТфОП/ISDN

Передача сигналов между MSC и подсистемой базовых станций осуществляется через систему ОКС№7 (уровни MTP, SCCP и прикладную подсистему базовых станций BSSAP,

Base Station Subsystem Application Part). Подсистему BSSAP можно разделить на две подсистемы: прикладную подсистему управления базовыми станциями (BSSMAP) и прикладную подсистему прямой передачи (DTAP).

Для поддержки сотовых сетей стандарта GSM на прикладном уровне была установлена подсистема мобильных приложений MAP (Mobile Application Part) интеллектуальной сети. Подсистема MAP обеспечивает взаимодействие сетевых компонентов (таких как MSC, OMC, AUC, BSC, регистры HLR, VLR, EIR), а также взаимодействие с сетями фиксированной связи, что позволяет передавать информацию между различными элементами сети при помощи каналонезависимой сигнализации. Сигнализация MAP используется при изменении информации о местоположении абонентов, передаче соединения между сотами (хэндовер, handover), роуминге, аутентификации, маршрутизации входящих вызовов и пересылке сообщений SMS. Подсистема MAP использует также как и подсистема INAP интеллектуальной сети через TCAP, SCCP и MAP (см. рис. 20.3 в главе 20 стек протоколов ОКС№7 для интеллектуальной сети). Хэндовер позволяет продолжать разговор, когда мобильная станция пересекает границы соты и перемещается в соседнюю. Роуминг- это функция предоставления услуг сотовой связи одного оператора в системе другого оператора. Упрощенная схема организации роуминга может быть представлена в следующем виде. Абонент сотовой связи, оказавшись на территории другого оператора, допускающего реализацию роуминга, инициирует вызов обычным образом, как если бы он находился на территории оператора, к которому он приписан.

Подсистема SCCP выполняет те же дополнительные возможности при работе через подсистему MTP, что и в интеллектуальной сети.

- расширяет функции сетевого уровня подсистемы MTP - третьего уровня модели OSI;
- обеспечивает работу служб передачи данных без установления соединения и служб с установлением соединений;
- обеспечивает гибкие механизмы управления маршрутизацией;
- обеспечивает управление подсистемой SCCP;
- осуществляет расширение адресации.

Подсистема управления соединением сигнализации SCCP состоит из тех же функциональных блоков:

- служба передачи сообщений с установлением и без установления соединения;

- управление маршрутизацией SCCP (SCRC);
- управление подсистемой SCCP (SCMG).

В подсистеме MAP задействован только режим без установления соединения подуровня управления соединением сигнализации SCCP. Согласно стандарту GSM, для маршрутизации так же, как и в интеллектуальной сети (глава 20) используется управление маршрутизацией SCCP (SCRC) по номерам подсистем SSN и по глобальным заголовкам GT. SSN в GSM присваиваются не отдельным услугам (как в интеллектуальной сети), а отдельным устройствам (коммутатору MSC, регистрам HLR, VLR, AUC, подсистеме BSS и др.). Номера подсистем могут использоваться в GSM из зарезервированного глобального стандартизированного международными организациями диапазона или из части национального незарезевированного диапазона. Номера глобальных подсистем SSN для маршрутизации на подуровне SCCP (SCCP Sybsystem Numbers), назначены Альянсом 3GPP и в MAP используются следующие:

- регистр HLR – 00000110;
- регистр VLR – 00000111;
- MSC – 00001000;
- регистр AUC;
- регистр EIR – 00001001 и др.

Покажем для иллюстрации пример использования маршрутизации по глобальным адресам в GSM. Требуется передать сообщение об изменении местоположения абонента из VLR в стране А в регистр HLR страны Б. В сообщении содержится адрес пункта сигнализации DPC международного коммутационного центра страны А, который предоставляет свои таблицы маршрутизации. Также в сообщении содержится глобальный заголовок регистра собственных абонентов HLR (адрес по стандарту E.164). В передаваемом сообщении содержится глобальный адрес вызываемой стороны, по которому можно идентифицировать получателя SCCP-сообщения. Международный коммутационный центр страны А устанавливает адрес пункта сигнализации DPC международного коммутационного центра страны Б, в таблице маршрутизации которого имеются данные для перевода глобального заголовка получателя в код пункта сигнализации и номер подсети (DPC+SSN). Только на последнем участке маршрутизация проводится по SSN, а на предыдущих маршрутизаторах - по глобальным заголовкам.

Управление подсистемой SCCP, приведенное в главе 20 для интеллектуальной сети,

аналогично и для GSM. Отличаются только используемые подсистемы пользователя. .

В таблице 22.1 приведено краткое описание некоторых протоколов ОКС№7, используемых в узлах GSM на различных интерфейсах.

Таблица 22.1. Интерфейсы и протоколы GSM-сети

Интер-фейс	Узлы GSM	Описание функции
A	BSS- MSC	A- интерфейс между подсистемой BSS (MS, BTS, BSC) и MSC. Он отвечает за резервирование и выделение достаточных радиоресурсов мобильным станциям (MS) и управляет мобильными абонентами. Этот интерфейс использует BSSAP- протоколы (BSSMAP и DTAP)
B	MSC- VLR	Это внутренний MAP- протокол, поскольку часто VLR встроен в MSC
C	GMSC- HLR	Любой звонок извне GSM-сети (например, из ТфОП на MS), должен использовать этот протокол MAP C-интерфейса. Кроме того, MSC может передавать тарифную информацию после завершения соединения
D	HLR- VLR	Используется для обмена информацией между HLR и VLR сообщениями MAP
E	MSC- MSC	Используется для обмена данными MAP между MSC
F	MSC- EIR	Используется для получения из регистра EIR сообщения MAP, указывающего на статус мобильного оборудования (украденное, потерянное и др.). Мобильное оборудование имеет международный идентификатор IMEI
G	VLR-VLR	Используется для передачи сообщений MAP, например, при роуминге

На рис. 22.3 приведены протоколы ОКС№7 для участка сети GSM, состоящего из двух мобильных центров коммутации MSC.

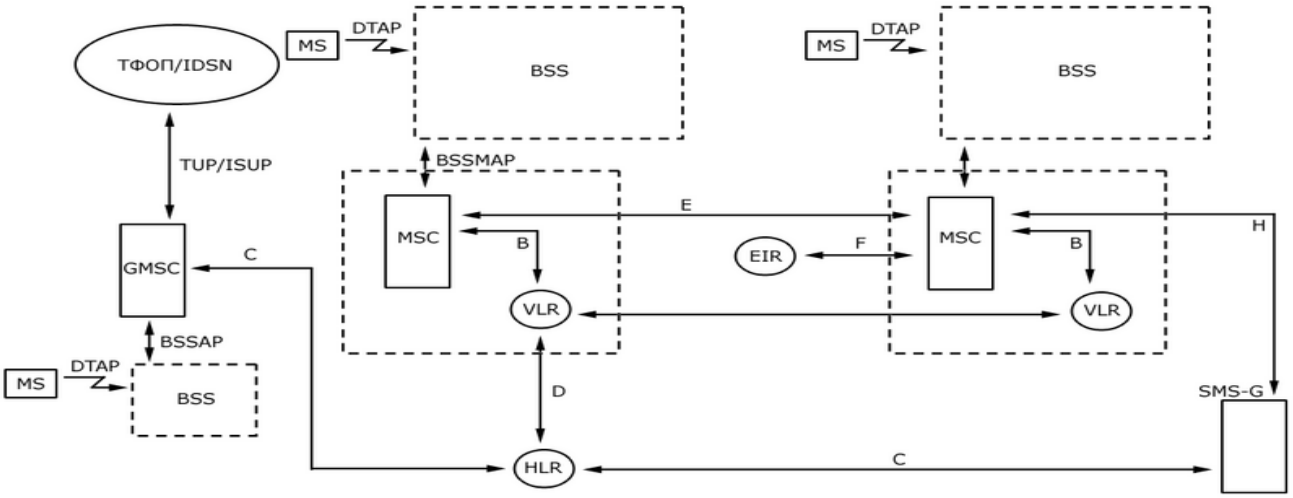


Рис. 22.3. Протоколы ОКС№7 для участка сети GSM, состоящего из двух мобильных центров коммутации MSC

22.2. Пример обработки вызова мобильной станции из ТфОП/ISDN и управление мобильностью

Рассмотрению подлежит алгоритм последовательности событий при обработке вызова оконечного мобильного устройства, а также последовательность сообщений при перемещении мобильной станции из зоны действия одного гостевого регистра в зону действий другого.

22.2.1. Вызов мобильной станции из ТфОП/ISDN и обеспечение защиты приватных данных местоположения абонента-роумера

На рис. 22.4 приведена диаграмма обмена сообщениями при установлении вызова мобильной станции из ТфОП/ISDN. В сообщении 1 вызывающий абонент через ТфОП/ISDN отправляет начальное адресное сообщение IAM подсистемы ISUP ОКС№7. В адресную часть этого сообщения входит международный номер ISDN вызываемой мобильной станции MSISDN (Mobile station international ISDN number). Этот номер связан не с определенным устройством, а с модулем SIM, принадлежащим пользователю и является мобильным абонентским номером. Этот номер состоит из кода страны, адреса сетевого поставщика услуг и регистра HLR и номера абонента. Сеть ТфОП/ISDN через ОКС№7 маршрутизирует это сообщение шлюзу GMSC (сообщение 2). Шлюз GMSC на основании MSISDN определяет регистр HLR домашней наземной части сети GSM. Сообщение 3 подсистемы MAP от GMSC в HLR служит для определения вызываемой мобильной станции MS. Это сообщение ОКС№7 MAP по интерфейсу C содержит в качестве параметра идентификатор IMSI. В регистре HLR содержится информация о местоположении вызываемой MS (указан адрес

регистра VLR). Вызываемая станция MS может находится в домашней или гостевой сети. В настоящем примере рассматривается случай ее расположения в гостевой сети. Следующее сообщение 4 подсистемы MAP из HLR домашней сети в VLR гостевой сети запрашивает роуминговый номер вызываемой мобильной станции MSRN (Mobile Station Roaming Number). Использование MSRN вызвано необходимостью скрытия местоположения абонента, которое является приватной информацией. Регистр VLR назначает номер MSRN из пула свободных номеров. Этот номер является временным и действует только до окончания установления соединения и устанавливается на основании международного идентификатора мобильного абонента IMSI. MSRN включает гостевой код страны, текущий центр коммутации MSC. Регистр VLR пересылает присвоенный временный номер MSRN в сообщении MAP по интерфейсу D в HLR домашней сети (сообщение 5). Далее MSRN пересылается в шлюз GMSC (сообщение 6). Теперь шлюз GMSC отправляет сообщение на установление соединения IAM подсистемы ISUP в текущий MSC (сообщение 7) . В адресной части IAM содержится полученный номер MSRN, включающий адрес MSC. Теперь, когда входящий вызов достиг нужного MSC, определяется идентификатор IMSI и дальнейшие процедуры протокола MAP ОКС№7 не требуются. Номер MSRN возвращается в пул для использования при дальнейших вызовах.

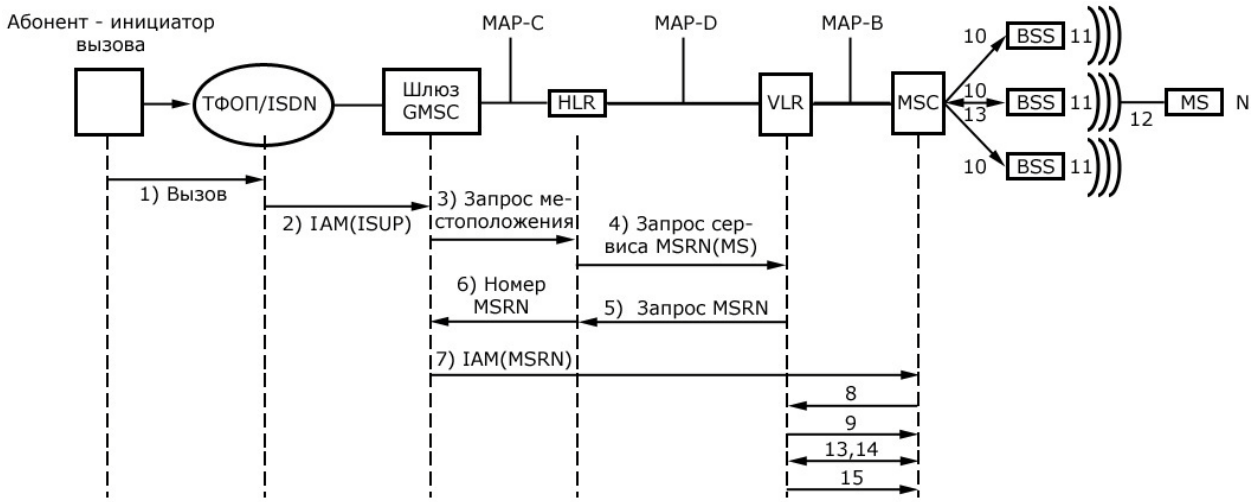


Рис. 22.4. Диаграмма обмена сообщениями при установлении вызова мобильной станции из ТфОП/ISDN

Начиная с этого места, за все дальнейшие шаги отвечает центр MSC. Прежде всего, он запрашивает из регистра VLR информацию о текущем состоянии мобильной станции (сообщение 8). Если мобильная станция доступна, центр MSC инициирует

широковещательным сообщением 10 ее поиск во всех своих ячейках (поиск одной нужной ячейки забрал бы слишком много времени). Станции BTS подсистемы BSS посылают широковещательное сообщение 11 (PAGE) подсистемы BSSAP на мобильную станцию. После ответа (12) регистр VLR должен произвести (13,14) проверку безопасности (установить шифрование и т.п.). Затем регистр VLR посылает сигнал об установке соединения с мобильной станцией центру MSC (15).

Если мобильная станция отвечает сообщением ALERT протокола DTAP, обслуживающий центр MSC отправляет сообщение ANM подсистемы ISUP через шлюз GMSC назад коммутатору вызывающей стороны в сети ТфОП/ISDN.

22.2.2. Управление мобильностью

Как было показано на диаграмме (рис. 22.4) в сообщении 4 HLR запрашивает MSRN на основании входящего в него сообщения IMSI. В гостевой сети, кроме IMSI роумера, содержатся также данные аутентификации (индивидуальный ключ абонента и другая информация). При перемещении MS из области действия одной VLR в область действия другой VLR, производится обновление этой информации в новом VLR и в домашнем HLR. На рис. 22.5 показана диаграмма последовательности сообщения протокола MAP при перемещении MS из зоны действия регистра VLR-A в зону действия VLR-B.

В сообщении 1 (sendidentification) протокола MAP по интерфейсу G производится запрос идентификационных данных из предыдущего регистра VLR-A, в области обслуживания которого находилась последний раз мобильная станция. В качестве аргумента в этом сообщении содержится временный идентификатор местоположения мобильного абонента TMSI, Temporary Mobile Subscriber Identity (см. глава 21, разд. 21.4.3.). В сообщении 2 VLR-B получает идентификационные данные этой MS (идентификатор IMSI, коды RAND, SRES и др.). В случае неудачи эти данные извлекаются из регистра HLR с помощью другой команды протокола MAP (sendAuthenticationInfo).

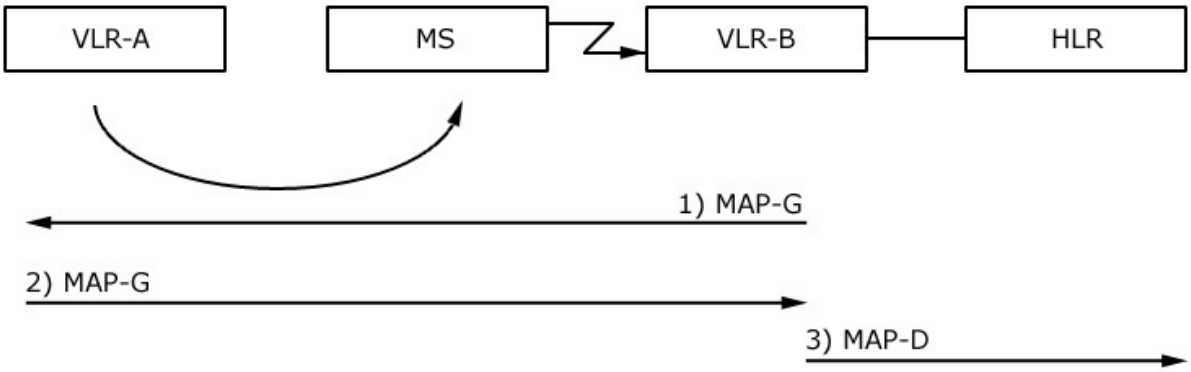


Рис. 22.5. Диаграмма последовательности сообщений протокола MAP при перемещении MS из зоны действия одного VLR в зону действия другого VLR

Получив в сообщении 2, все аутентификационные данные в случае вызываемой или вызывающей станции MS производится процедура аутентификации и шифрования. После успешного завершения этой процедуры производится по команде протокола MAP (“updateLocation”) по интерфейсу G смена параметров местоположения LAI и временного идентификатора местоположения TMSI. Параметр TMSI используется вместо IMSI из соображений приватности местоположения абонента. Передача IMSI, также как и индивидуального ключа Ki по радиоучастку не разрешается. (Допускается передача IMSI только один раз при первоначальной регистрации MS). Передача нового TMSI производится в зашифрованном виде. Новое LAI и TMSI передается из VLR-B в HLR (сообщение 3.).

22.3. Принцип иерархии федеральной сети общего пользования GSM

Федеральная сеть GSM представляет иерархическую структуру, принцип построения которой приведен на рис. 22.6. Первый уровень включает мобильные центры коммутации MSC, шлюз мобильного центра коммутации.

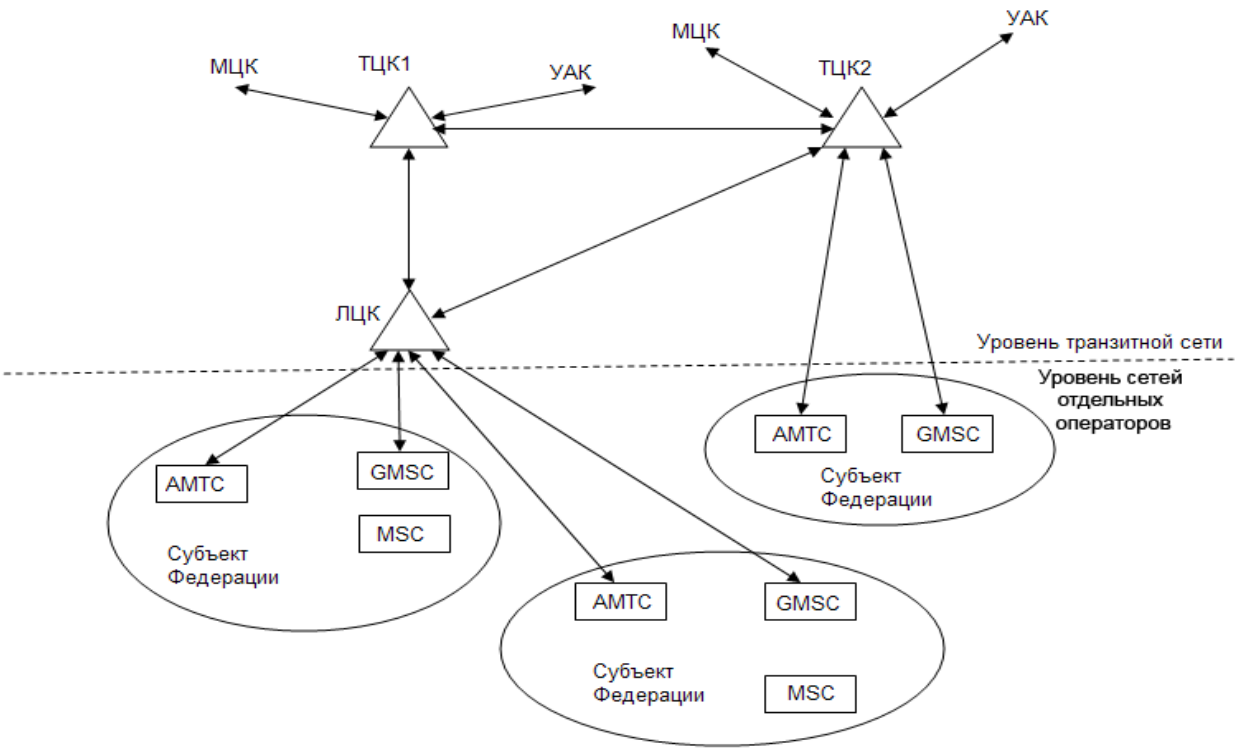


Рис. 22.6. Принцип иерархии федеральной сети общего пользования GSM

Взаимодействие сети GSM со стационарной сетью ТфОП осуществляется через шлюз мобильного центра коммутации GMSC подключением к АМТС (основной вариант) и к АТС при значительном тяготении нагрузки абонентов на местном уровне. Второй уровень иерархии GSM- транзитная сеть, представляющая собой транзитные центры коммутации (ТЦК), выполняющие для мобильных абонентов те же функции, что и УАК для ТфОП. Все ТЦК соединены между собой по полносвязной схеме. При взаимодействии федеральной сети GSM с фиксированной сетью ТфОП на международном уровне возможны соединения мобильной станции MS с телефонным аппаратом (ТА) стационарной сети ТфОП: MS-MSC-GMSC-ТЦК-УАК-АМТС-АТС-ТА.

Кроме ТЦК уровень транзитной сети может включать также локальные центры коммутации (ЛЦК). ЛЦК является промежуточным уровнем иерархии федеральной сети GSM. ЛЦК является узлом доступа к транзитной сети и соединяется не менее чем с двумя ТЦК. В этом случае взаимодействие мобильной станции и стационарного телефонного абонента при междугородней связи осуществляется по схеме:

MS-MSC-GMSC-ЛЦК-ТЦК-УАК-АМТС-АТС-ТА.

22.4. Принцип построения системы ОКС№7 России

На рис. 22.7 показан иерархический принцип построения системы ОКС№7 РФ,

которая является составной частью сетей связи общего пользования страны ТфОП/ISDN, IN и GSM.

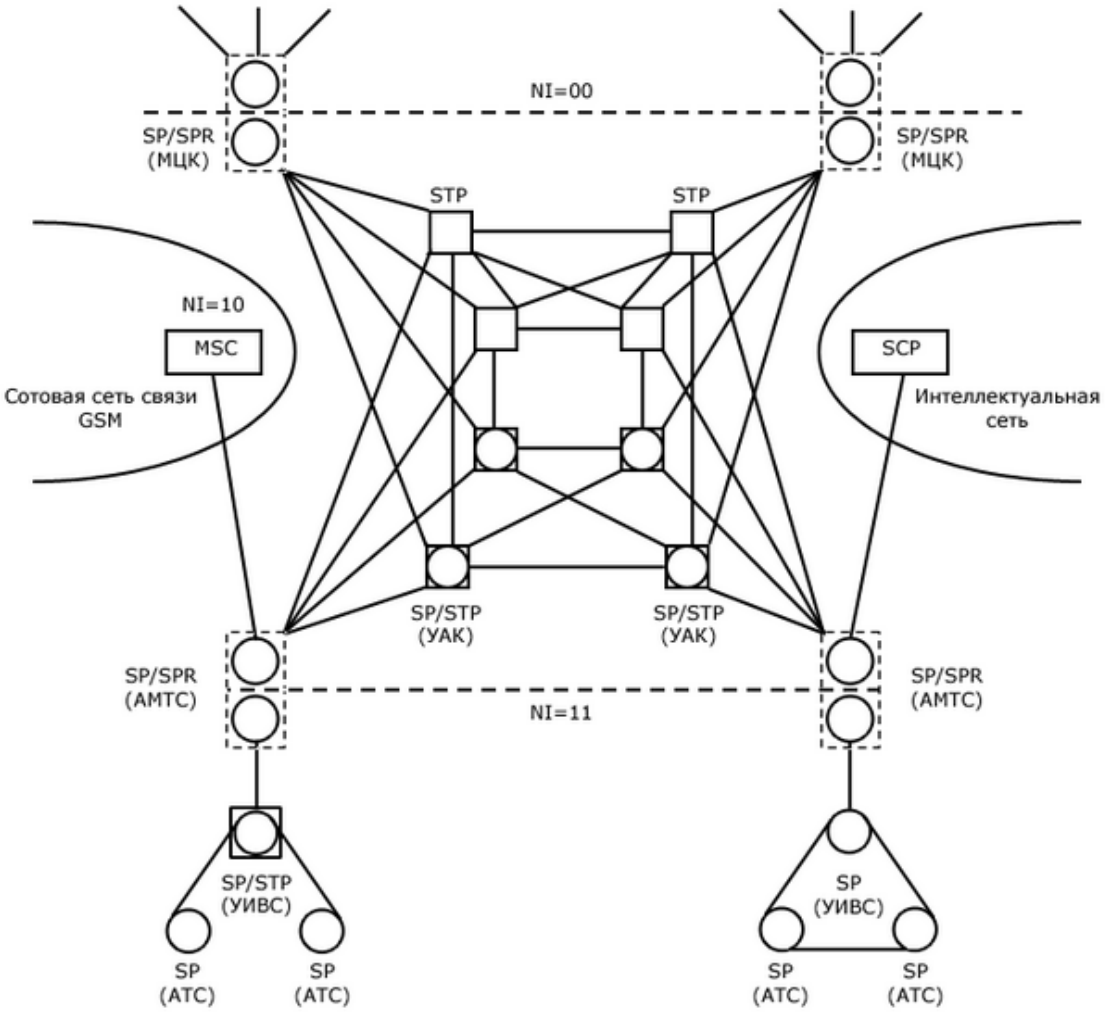


Рис. 22.7. Принцип построения системы ОКС№7 России

На рисунке приняты следующие обозначения:

MSC - центр коммутации мобильной сети связи;

SCP - пункт управления услугами интеллектуальной сети связи.

В поле индикатора сети NI заголовка MSU подсистемы сообщений MTP идентифицируется следующим образом каждый из этих уровней. Международная сеть - 00, междугородная сеть - 10, местная сеть - 11.

Такое построение сетей ОКС№7 РФ требует трансляцию номеров в подсистеме SCCP. Пункт сигнализации с функцией переприема теоретически обеспечивает суммарную емкость 2^{28} пунктов сигнализации. Однако практический предел емкости сети сигнализации снижен

за счет необходимости использования нескольких пунктов сигнализации междугородной сети для разных операторов связи. Пункт сигнализации с функцией переприёма организован на междугородном центре коммутации АМТС или на международном центре коммутации МЦК. На рис. 22.7 такой сигнальный пункт с функцией переприёма сообщений SCCP обозначен через SPR (Signaling Point Relay).

Междугородная сеть ОКС№7 России представляет собой совокупность пунктов сигнализации SP с функцией переприема (SP/SPR), построенных на базе АМТС и взаимодействующих через сеть транзитных пунктов сигнализации STP, созданных на базе узлов автоматической коммутации (УАК) или на базе выделенного оборудования. Каждый SP/SPR для обеспечения требований к MTP по качеству обслуживания взаимодействует, по крайней мере, с двумя STP.

На рисунке 22.7 не указаны многие устройства, включающие ОКС№7 (транзитные и локальные центры коммутации транзитного уровня федеральной сети GSM России, домашний и гостевой регистры уровня сетей отдельных операторов GSM и др.).

Между местной и междугородной сетью РФ устанавливается шлюз, который строится на базе автоматической междугородной станции (АМТС) с двойной нумерацией пунктов сигнализации. Это означает, что в оборудование АМТС включено два пункта сигнализации - один с нумерацией в междугородней сети (NI=10) и другой с нумерацией в местной сети (NI=00). Между междугородной и международной сетью РФ также включено два пункта сигнализации — один с нумерацией междугородной сети NI=10, а другой с нумерацией международной сети NI=00.

22.5. Информационная безопасность ОКС№7

Во многих работах по информационной безопасности общеканальной сигнализации ОКС№7 [72-73] отмечается ее уязвимость по отношению к атакам нарушения маршрутизации, приводящим к нарушению работы сетей связи общего пользования (ССОП). Специалисты фирмы Cisco отмечают, что в их оборудовании ОКС№7 не предусмотрены механизмы аутентификации для защиты от атак типа "отказ в обслуживании" DoS [72]. Настоящий раздел посвящен описанию ущерба от таких атак, наносимого работе ССОП РФ (ТфОП/ISDN, GSM и интеллектуальных сетей связи IN).

22.5.1. Архитектура сетевой безопасности ОКС№7

В приложении А приведены общие положения по архитектуре сетевой безопасности в соответствии с рекомендацией ITU-T X.805, которые могут быть применимы к конкретной технологии сети связи. В настоящем разделе приводится архитектура сетевой безопасности

для одной из таких технологий - системы сигнализации ОКС№7 [74,75].

22.5.1.1. Уровни безопасности ОКС№7

Приведенные в X.805 способы обеспечения ИБ относятся и к группе оборудования ОКС№7, которое в соответствии с общими положениями по архитектуре сетевой безопасности распределены по уровням безопасности (Security Layers). Учитывая особенности ОКС№7, способы обеспечения ИБ рассматриваются относительно двух уровней безопасности: уровень безопасности инфраструктуры (Infrastructure Security) и уровень безопасности приложений (Application Security). Взаимосвязь уровней безопасности основана на иерархическом принципе. Уровень безопасности инфраструктуры обеспечивает уровень безопасности приложений.

Уровень безопасности инфраструктуры относится к устройствам ОКС№7: оконечным, промежуточным и транзитным пунктам сигнализации. Все приведенные способы обеспечения ИБ в X.805 могут применяться ко всем уровням эталонной модели OSI уровня безопасности инфраструктуры ОКС№7.

Способы обеспечения ИБ ОКС№7 на уровне безопасности инфраструктуры предназначены для того, чтобы уменьшить уязвимость к атакам, соответствующим угрозам ИБ. Способы обеспечения ИБ ОКС№7 на уровне безопасности инфраструктуры позволяют защитить уязвимость на всех уровнях ОКС№7. Оборудование трех уровней ОКС№7 всех типов пунктов сигнализации (оконечный, промежуточный, транзитный) подвержены атакам соответствующих угроз ИБ.
К ним относятся:

- физический, канальный и сетевой уровни подсистемы передачи сообщений MTP;
- сетевой уровень подсистемы управления соединением сигнализации SCCP.

Последствия воздействия угроз ИБ на четвёртом (прикладном) уровне одного пункта сигнализации ОКС№7 уровня безопасности инфраструктуры отражаются на работе только этого пункта сигнализации. В общем виде можно выделить две группы пользовательского уровня ОКС№7. К первой из них относятся пользователи, для которых большинство функции связи определено выбором информационного канала в сети ТфОП/ISDN или в сети GSM (на участке от мобильной станции коммуникации и шлюзом к ТфОП). Такая подсистема ISUP или TUP используется для межстанционной сетевой сигнализации. К другой группе относится пользователи, для которых функции не определены выбором информационного

канала. К подсистемам таких пользователей на сети связи ОП относятся:

- подсистема пользователей мобильной связи стандарта GSM (MAP);
- подсистема пользователей интеллектуальной сети (INAP).

К уровню безопасности инфраструктуры относится и оборудование ССОП (ТфОП/ISDN, GSM, IN), составной частью которой является оборудование ОКС№7. В ТфОП/ISDN оборудование ОКС№7 входит в коммуникационные станции местной сети связи, междугородной и международной сети. В GSM оборудование ОКС№7 входит в центр коммутации мобильной сети связи, домашний и гостевой, транзитный и локальный центр коммутации. В IN оборудование ОКС№7 входит в узел коммутации услуг и в узел управления услугами. Программно-аппаратная неисправность одного из пунктов сигнализации ОКС№7 является маловероятной.

22.5.1.2. Плоскости безопасности ОКС№7

Способы обеспечения ИБ относятся к функциям ОКС№7, которые в соответствии с общими положениями по архитектуре сетевой безопасности в рекомендации X.805 называются плоскостями безопасности (Security Plane). Плоскости безопасности ОКС№7 делятся на плоскость безопасности управления и плоскость безопасности транспортной сети. Плоскость безопасности управления относится к защите функций эксплуатации и технического обслуживания OAM. Примером таких функций в ОКС№7 является управление звеньями сигнализации, которое может быть разделено на процесс активизации и деактивизации звена сигнализации (канала). Активизация является процессом создания канала для передачи сообщений сетевого уровня MTP. Обслуживающий персонал выполняет этот процесс путём вызова команд из интерфейса OAM, чтобы осуществить запрос об активизации канала. Когда канал отрегулирован на канальном уровне MTP и прошел тестирование он объявляется доступным для переноса сигнального трафика. Дезактивизация выводит канал из рабочего состояния, делая его недоступным для переноса сигнального трафика. Подобно активизации, этот процесс инициализируется обслуживающим персоналом путём вызова команд из интерфейса OAM. Нарушение ИБ ОКС№7 может быть осуществлено злоумышленником путём ложной активизации или дезактивизации канала. При этом ущерб работе ССОП не будет высоким. Плоскость безопасности транспортной сети относится к защите всех четырёх уровней ОКС№7 при воздействии намеренных угроз нелегитимного использования основных функций. Ниже приводятся краткое описание этих функций ОКС№7, а также общие положения по наибольшему ущербу в сетях связи ОП при реализации этих угроз.

Подсистема пользователя ISUP совместно с подсистемой передачи сообщений MTP обеспечивает соединение со стационарными абонентами ССОП. Нарушение ИБ ОКС№7 при нелегитимном воздействии на функцию ISUP может приводить к отказу в установлении соединений, проходящих через конкретный пункт сигнализации, которому принадлежит эта подсистема пользователя. Нарушение ИБ ОКС№7 при нелегитимном воздействии на функцию ISUP приводит к отказу в установлении соединений мобильным станциям, приписанных только к этому оборудованию.

Подсистема пользователя MAP выполняет функцию отслеживания местоположения абонента, роуминга, доставки коротких текстовых сообщений SMS и др. Нарушение ИБ ОКС№7 при нелегитимном воздействии на эти функции GSM может привести к отказу в установлении соединений с абонентами-роумерами, передаче SMS, приписанных к одному центру коммутации GSM .

Подсистема INAP выполняет функцию предоставления услуги пользователю путем обмена сообщениями между двумя узлами интеллектуальной сети SCP и SSP. Приведем принцип выполнения этой функции на упрощенном примере предоставления услуги «Приплата» (PRM, Premium Rate). Все сообщения между SCP и SSP можно разделить на две группы:

- пересчет кода и номера услуги в адрес абонента услуги (юрист, врач и др.);
- определение размера оплаты и распределение оплаты между оператором связи, поставщиком услуги и пользователем услуги.

Нарушение ИБ ОКС№7 при нелегитимном воздействии на эти функции может привести к отказу в предоставлении услуги IN, неправильном распределении оплаты за услугу только абонентов, пользующихся этой интеллектуальной платформой.

Уровни MTP с первого по третий включают в себя функции передачи информации от одного пункта сигнализации к другому.

Функционирование каналов передачи сообщений обеспечивается комбинацией подсистем первого уровня (MTP1) и второго уровня (MTP2).

Нарушение ИБ ОКС№7 при нелегитимном воздействии на эти функции может привести к отказу только одного звена сигнализации.

Подсистема сетевого уровня MTP3 по выполнению функций обработки сообщений сигнализации. Эта функция производит маршрутизацию сообщений для соответствующих сетевых адресатов. Если принимающий узел не является пунктом назначения, то MTP3 выполняет функцию маршрутизации (т.е. узел является транзитным STP). Если

принимающий узел является пунктом назначения, то используется функция доставки принятых сообщений соответствующей подсистеме пользователя или функциям управления сетью сигнализации. Использование нарушителем функций маршрутизации для нарушения таблицы маршрутизации является маловероятным, хотя реализация такой угрозы могло бы привести к отказу в предоставлении соединений и/или услуг одновременно для большого числа абонентов ССОП, обслуживаемых данным пунктом сигнализации. Подсистема сетевого уровня MTP3 по выполнению функций управления сетью сигнализации. Эти функции с помощью набора специальных сообщений и процедур производят обработку отказов в сети таким образом, чтобы информационные сообщения могли достигать своих адресатов, если это возможно. Эти процедуры координируют ресурсы ОКС№7, которые становятся доступными или недоступными. Отказ звена сигнализации одного пункта сигнализации или отказ пункта сигнализации может повлечь недоступность проходящих через него маршрутов сигнализации к пункту сигнализации назначения, что в свою очередь может вызвать изменение таблицы маршрутизации и в других пунктах сигнализации ОКС№7. Последствием такой атаки может быть вывод из рабочего состояния части сети связи общего пользования страны.

22.5.2. Атаки «отказ в обслуживании» DoS в ОКС№7

Для каждого уровня безопасности соответствует каждая плоскость безопасности. Каждая такая пара безопасности (уровень и плоскость) представляет область безопасности, в которой способы обеспечения безопасности применяются для защиты от угроз безопасности. Из предыдущего раздела следует, что уровень и плоскость безопасности включает большое число составных частей оборудования ОКС№7 и выполняемых ими функций, каждые из которых могут быть подвержены воздействию различных видов атак, т.е. реализованных намеренных угроз. Все это показывает, что число возможных атак в ОКС№7 настолько большое, что нет необходимости, да и возможности в анализе их всех. Поэтому практическую целесообразность представляет анализ таких угроз в ОКС№7, которые наиболее чувствительны с точки зрения нанесения большого ущерба при их реализации. Приведенный выше анализ архитектуры сетевой безопасности ОКС№7 показывает, что таким угрозам подвержен уровень сетевой безопасности *инфраструктура* и *плоскость* сетевой безопасности в той части транспортной сети, которая выполняет функцию управления сетью сигнализации на сетевых уровнях ОКС№7. Управление сетью сигнализации подразделяется на выполнение функций управления информационными потоками и управления маршрутами. Функция управления информационными потоками обеспечивает трансляцию информационных потоков

сигнализации, которые представляют собой сообщения подсистемы ISUP и подсистем пользователей через SCCP (MAP, INAP и др.). Функция управления информационными потоками состоит в перемещении информации к адресату в случае повреждений или перегрузок в ОКС№7 с наименьшими возможными потерями. Функция управления маршрутами обеспечивает обмен информацией между пунктами сигнализации для коррекции таблиц маршрутизации. Как только происходит событие, которое влияет на доступность маршрутов, функция управления маршрутами, посылает сообщения оповещения остальным пунктам сигнализации об изменении маршрутизации. Нарушение ИБ ОКС№7 при отправлении ложных сообщений управления маршрутами может создать нелегитимную коррекцию таблицы маршрутизации. В результате система управления информационными потоками направляет в пункты сигнализации нелегитимные сообщения коррекции информационных потоков.

Функция управления маршрутами с помощью специальных сообщений MTP3 обеспечивает выполнение функций управления информационным потоком при полной или ограниченной доступности сигнальных маршрутов. Нарушение ИБ ОКС№7 при отправлении ложных сообщений управления информационным потоком может создать нелегитимную недоступность или нелегитимную доступность сигнальных маршрутов. Результатом нарушений ИБ ОКС№7 при выполнении функций управления маршрутами и функций управления информационным потоком может быть отказ в обслуживании одновременно большого числа пользователей сетями связи общего пользования (ТфОП/ISDN, GSM, IN), являющихся абонентами двух и более оконечных узлов сетей ТфОП/ISDN и GSM. Всё это приводит к существенному повреждению сетей связи ОП, составной частью которых является ОКС№7.

Подсистема управления соединением SCCP расположена в стеке уровней ОКС№7 над подсистемой MTP и обеспечивает дополнительные функции сетевого уровня в части управления прикладными системами (в сетях GSM, интеллектуальных сетях и др.). Подсистема SCCP вместе с подсистемой MTP3 соответствует третьему (сетевому) уровню ОКС№7 и при этом дает возможность передавать информацию, не связанную с информационным каналом.
Нарушение ИБ ОКС№7 в результате передачи ложных сообщений управления подсистемой SCCP может привести к нелегитимному отказу в обслуживании SCCP, подсистем (MAP, INAP, OMAP), локальных подсистем (центр коммутации мобильной сети GSM, домашний и гостевой регистры GSM и др.). Всё это может привести к отказу ССОП в обслуживании пользователей по предоставлению им соединений.

Для реализации таких угроз нарушителем используются функции подсистем MTP и SCCP сетевого уровня ОКС№7. Уровень ущерба, наносимого работе ССОП атаками «отказ в обслуживании» DoS (Denial of Service), определяется теми функциями MTP и SCCP, которые нелегитимно использует нарушитель на различных участках смежных пунктов сигнализации ОКС№7. Последствия нарушения работы ССОП зависят также от топологии этих сетей: уровней иерархического построения, схем резервирования и взаимодействия. Приведем примеры, реализующие эти атаки и их последствия.

22.5.2.1. Примеры последствий воздействия атак DoS нарушения маршрутизации ОКС№7

Учитывая сложную топологию ССОП, последствия атак DoS нарушения маршрутизации ОКС№7 на ТфОП/ISDN, GSM и интеллектуальную сеть связи IN рассмотрим на примерах структур отдельных фрагментов ОКС№7. На рис. 22.8 приведён фрагмент ОКС№7, включающий АМТС, УАК, шлюз мобильного центра коммутации GMSC сети GSM, узел исходящей и входящей связи УИВС. Такая схема соответствует топологии ССОП России.

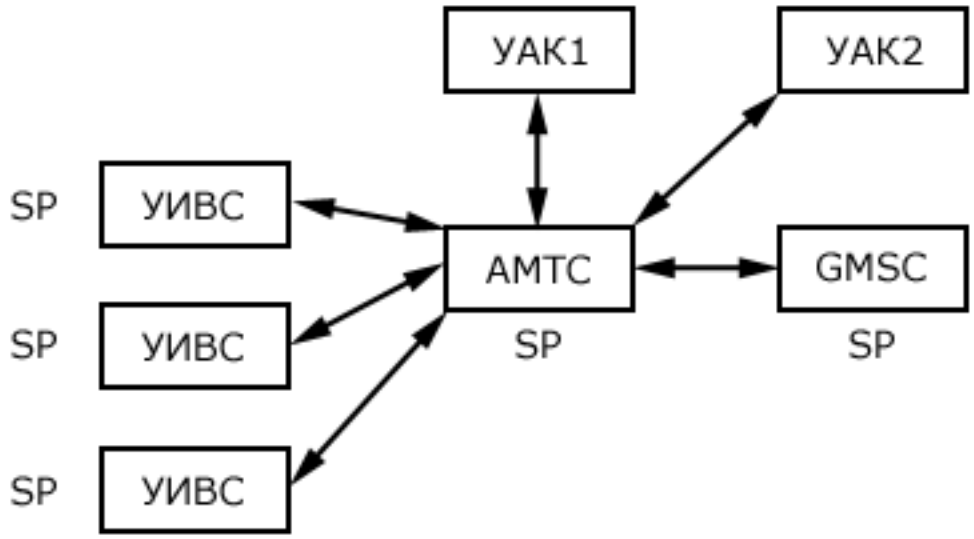


Рис. 22.8. Фрагмент сети ОКС№7

К основным функциям сетевого уровня ОКС№7, нелегитимное использование которых злоумышленником представляет угрозу нарушения маршрутизации, относятся:

- функции MTP: запрет передачи (сообщение TFP); недоступность подсистемы

пользователя (сообщение UPU); перегрузка пучка звеньев сигнализации (сообщение TFC); ограничение передачи (сообщение TFR); переключение звена сигнализации (сообщения COO, ECO) и др.;

- функции SCCP: запрет доступа (сообщение SSP), подсистема перегружена (сообщение SSC) и др.

Ниже приведены примеры последствий реализации угроз нарушения маршрутизации сети ОКС№7 при использовании злоумышленником одной из функций: управление сетью сигнализации на третьем уровне MTP с помощью нелегитимного сообщения "запрет передачи" (сообщение TFP), т.е. недоступности определенного пункта сигнализации.
Пример1. Нарушитель создаёт в пункте SP (AMTC) нелегитимное сообщение TFP о недоступности пунктов сигнализации SP в УИВС. Эти сообщения передаются из AMTC в УАК1, УАК2 и GMSC. Последствием такой атаки DoS является отказ всем входящим вызовам от пользователей ТфОП/ISDN и GSM в установлении соединений с абонентами всех АТС, подключённых к этим УИВС. При этом сохраняется возможность установления соединений внутри местной сети ТфОП/ISDN.
Пример2. Нарушитель создаёт в пункте SP (AMTC) нелегитимное сообщение TFP о недоступности пунктов сигнализации SP в обоих УАК. Эти сообщения передаются из SP в AMTC в любой SP в УИВС или в SP всех УИВС местной сети. Последствием такой атаки DoS является отказ пользователям АТС, подключённым к этим УИВС в установлении междугородних и международных соединений исходящим вызовам. Такой отказ относится к вызываемым стационарным аппаратам и мобильным станциям. Исключение составляют соединения с мобильными станциями, обслуживаемыми GMSC.
Пример3. Нарушитель создаёт в пункте SP (AMTC) нелегитимное сообщение TFP о недоступности пунктов сигнализации SP в GMSC. Это сообщение передаётся из SP в AMTC в любой SP в УИВС или в SP всех УИВС местной сети. Последствием такой атаки DoS является отказ пользователям АТС, подключённым к этим УИВС в установлении соединений исходящим вызовам к мобильным станциям, обслуживаемым через GMSC.
Пример 4. Нарушитель создаёт в пункте SP (AMTC) нелегитимное сообщение о недоступности пунктов сигнализации SP в обоих УАК. Эти сообщения передаются из SP в AMTC в SP в GMSC. Последствием такой атаки DoS является отказ мобильным станциям, обслуживаемыми через GMSC в установлении соединений исходящим междугородным и международным вызовам со стационарными аппаратами и мобильными станциями.
Пример 5. Нарушитель создаёт в пункте SP (AMTC) нелегитимное сообщение о недоступности всех смежных с ним пунктов сигнализации (в УАК1, УАК2, УИВСы, GMSC,

АМТСы внутри зоны) и передаёт их каждому из этих пунктов. Последствием такой атаки DoS является отказ в установлении всех видов соединений с абонентами зоны сети, обслуживаемой зоновой АМТС.

Следующие два примера последствий атак DoS приведены для фрагмента ССОП на рис. 22.9. Здесь показано взаимодействие локального центра коммутации (ЛЦК) уровня транзитной сети с двумя транзитными центрами коммутации (ТЦК1 и ТЦК2), со шлюзом GMSC и зоновой АМТС. Подробно принцип иерархии федеральной сети связи общего пользования стандарта GSM приводится выше в настоящей главе (раздел 22.3).

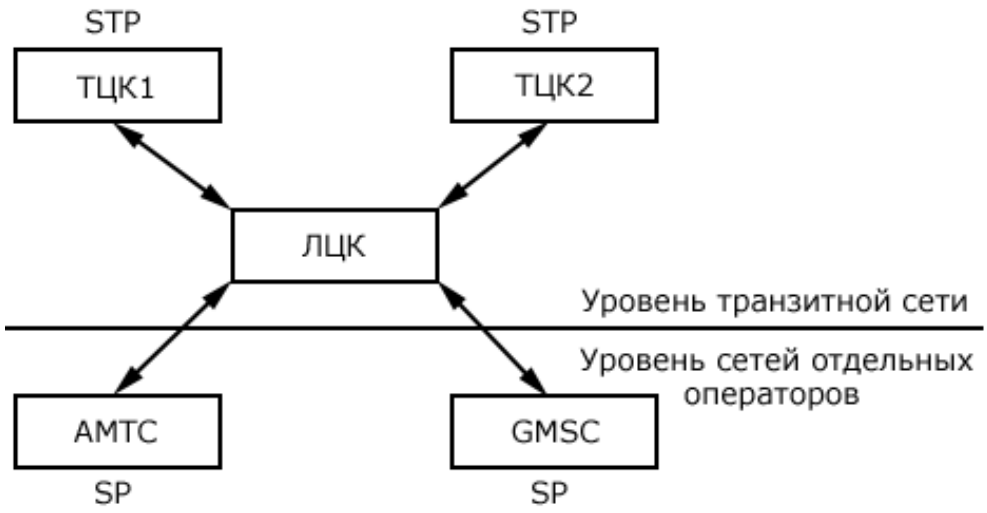


Рис. 22.9. Фрагмент сети ОКС№7

Пример 6. Нарушитель создает в пункте SP (ЛЦК) нелегитимные сообщения TFP о недоступности пунктов SP (ТЦК1 и ТЦК2). Эти сообщения передаются в пункты SP (АМТС) и SP (GMSC). Последствием такой атаки DoS является отказ вызовам на установление соединений через уровень транзитной сети GSM, исходящим от абонентов всех АТС зоны обслуживания АМТС и от мобильных станций, обслуживаемых станциями коммутации MSC через GMSC.

Пример 7. Нарушитель создает в пункте SP (ЛЦК) нелегитимное сообщение TFP о недоступности пунктов SP (АМТС). Это сообщение передается в пункты SP (GMSC). Последствием такой атаки DoS является отказ исходящим вызовам в установлении

соединений через уровень транзитной сети GSM от абонентов АТС зоны обслуживания АМТС с мобильными станциями, которые обслуживаются мобильными станциями коммутации через GMSC.

22.5.2.2 Результаты анализа архитектуры сетевой безопасности ОКС№7 при воздействии атаки DoS процедуры маршрутизации

Кратко сформулируем результаты анализа архитектуры сетевой безопасности ОКС№7 при воздействии атаки DoS процедуры маршрутизации.

- В результате нелегитимного использования функций сетевого уровня ОКС№7 по обновлению маршрутизации может быть нанесен значительный ущерб в работе сетей связи общего пользования (ТфОП/ЦСИС, СПС стандарта GSM, а также интеллектуальных сетей). Этот ущерб выражается в отказе установления соединении между пользователями (с предоставлением и без предоставления услуг интеллектуальной сети) и может относится одновременно к большому числу пользователей сетями связи общего пользования. Причиной таких последствий являются ложные сообщения обновления таблиц маршрутизации ОКС№7, отправляемые нарушителями.
- Зависимость риска ИБ от места атаки DoS в иерархической структуре ОКС№7. Структура ОКС№7 Единой сети электросвязи России построена на многоуровневой иерархической структуре в составе ТфОП/ISDN и в составе сети “МТТ” (“Межрегиональный Транзит Телеком”). Из примеров угроз DoS в ОКС№7 следует, что передача злоумышленником фиктивных сообщений обновления маршрутизации управления сетью сигнализации подсистемы передачи сообщений MTP (Message Transfer Part) может привести к различным последствиям нарушения выполнения маршрутизации. Наиболее уязвимыми с этой точки зрения являются участки сети ОКС№7 между пунктами сигнализации смежных уровней иерархии. Последствия атак DoS в ОКС№7 зависят от направления передаваемых злоумышленником сообщений. Передача таких сообщений подсистемы управления сетью сигнализации, как запрещение переноса трафика TFP (Transfer Prohibited) от пункта сигнализации ОКС№7 верхнего уровня иерархии к пункту сигнализации смежного нижнего уровня может приводить к прекращению обработки вызовов от абонентов, обрабатываемых узлом нижнего уровня иерархии.

  Приведем пример последствий такой атаки злоумышленника. Для этого достаточно

из зоновой АМТС хотя бы в одну из АМТС зоны передать два нелегитимных сообщения TFP о недоступности пункта сигнализации этой зоновой АМТС с двумя соединенными с ней пунктами сигнализации УАК. В результате пользователям этой АМТС зоны прекращается предоставление установления междугородных и международных соединений по исходящим от них вызовам. Передача этих сообщений от пункта сигнализации нижнего уровня иерархии к пункту сигнализации смежного верхнего уровня может приводить к прекращению выполнения функций по установлению соединений для входящих вызовов, обрабатываемых узлом нижнего уровня иерархии.

Если сообщения TFP от пункта сигнализации зоновой АМТС будут переданы в пункты сигнализации двух соединенных с ней УАК о недоступности пункта сигнализации АМТС этой зоны, то прекращается предоставление установления междугородных и международных соединений по входящим вызовам ко всем пользователям этой АМТС зоны.

- Для абонентов-роумеров сети GSM, требующий выполнение процедур защиты приватных данных их местоположения, риск ИБ из-за атак DoS в ОКС№7 выше по сравнению с абонентами в домашней сети. В результате посылки злоумышленником нелегитимных сообщений обновления маршрутизации для тех абонентов-роумеров гостевой сети, мобильные станции которых не смогли выполнить процедуру регистрации (см. разделы 21.4.3 и 22.2.2) последствия такой атаки DoS выражаются в отказе установления входящих и исходящих соединений. Это может иметь место при прекращении функционирования маршрута ОКС№7 между VLR, который ранее обслуживал данную MS абонента-роумера, и текущим VLR. При большом удалении их друг от друга по сети ОКС№7 и при пересечении нескольких уровней иерархии показатель риска, выраженный вероятностью атаки DoS выше для MS абонентов-роумеров. Другой показатель риска, (последствие атаки) при отказе в регистрации MS и отказе принятия на обслуживание гостевой сетью для абонентов-роумеров хуже, чем при отказе на установление или прием вызовов. При вызове удаленных от домашней сети абонентов-роумеров величина риска ИБ также может быть выше по характеристикам вероятности и последствий [76].
- Способ обеспечения ИБ «целостность данных» вместе с аутентификацией (подлинностью источника сообщений являются основными средствами защиты от этих угроз DoS ОКС№7, гарантируя при этом подлинность источника сообщений между пунктами сигнализации, а также то, что эти сообщения не были созданы или

заменены злоумышленником.

- Угрозам DoS ОКС№7 потенциально подвержены как абоненты фиксированной сети ТфОП/ISDN, так и пользователи мобильных станций сети GSM.
- Угрозы DoS ОКС№7 проявляются при фальсификации сообщений обновления маршрутизации подсистемы MTP3 и SCCP сетевого уровня ОКС№7.
- Реализация угроз DoS ОКС№7 может иметь место в результате фальсификации сообщений обновления маршрутизации между всеми смежными пунктами сигнализации.
- Нарушению маршрутизации от воздействия угроз DoS ОКС№7 подвержены смежные пункты сигнализации ОКС№7 с пунктом сигнализации, являющимся источником этих фальсифицированных сообщений обновления маршрутизации. Местом локализации при тестировании, а также местом защиты от воздействия угрозы являются эти пункты сигнализации.

Риск при реализации угроз DoS ОКС№7 в результате фальсификации указанных сообщений подсистем MTP3 и SCCP отражается на пользователях ССОП (ТфОП/ISDN, GSM, IN) в части:

- отказа в установлении соединения;
- отказа в предоставлении всех или определенных услуг интеллектуальной сети;
- ухудшения качества обслуживания.

Риск при реализации угроз DoS ОКС№7 может относится к следующим соединениям:

а) в ТфОП/ISDN – международным, междугородним или местным;
б) в GSM – внутри одного региона страны, между разными регионами страны, между мобильными абонентами разных стран;
в) между абонентами ТфОП/ISDN и абонентами GSM;
г) в сети GSM мобильных абонентов домашней и абонентов-раумеров.

д) в сети связи (см. глава 18) IP-телефонии для соединений абонентов ТфОП/ISDN через протокол SIP-T [77].

Заинтересованными в защите от угроз DoS ОКС№7 являются:

- пользователи в отношении доверия к сети и услугам, предоставляемым конкретным оператором/поставщиком услуг;

- операторы сетей и поставщики услуг в обеспечении защиты своих эксплуатационных и коммерческих интересов, в выполнении своих обязательств перед населением;
- органы государственной власти в выполнении директив и законов с тем, чтобы обеспечить готовность предоставления услуг и добросовестную конкуренцию.

В то же время следует отметить на наличие на сети ТфОП России большого количества коммутационного оборудования зарубежных производителей, что делает сложной задачу использования на эксплуатируемой сети механизмов аутентификации от таких атак DoS в ОКС№7. По прошествии более 20 лет после разработки, спецификации и реализации ОКС№7 можно было бы ожидать, что процедуры сетевого уровня работают хорошо. Однако один из разработчиков стандартов ITU-T на ОКС№7 (в работе [78], с. 2) отмечает случаи прекращения функционирования отдельных сегментов ТфОП по разным причинам недостаточной информационной безопасности подсистемы сетевого уровня системы сигнализации. В качестве объяснения этому указывается на сложности проблем, которые не позволили группе специалистов ITU-T успешно их решить.

ГЛАВА 23. Сети сотовой связи стандартов GPRS, EDGE и UMTS

GSM-сети, относящиеся ко второму поколению (2G), обеспечивают достаточно высокое качество передачи голоса, но позволяют осуществлять передачу данных с низкой скоростью (равную 14,4 Кбит/с и меньше). За последнее десятилетие наблюдается рост спроса пользователей на системы с более высокоскоростные соединения. Интерес пользователей к широкополосному доступу объясняется, в частности, распространением в Интернете контента и приложений, требующих широкополосного доступа ШПД. В таблице 23.1, взятой из материала Международного Союза Электросвязи, показано время, необходимое для загрузки контента на различных скоростях.

Таблица 23.1. Время загрузки контента на различных скоростях

Контент	256 кбит/с	2 Мбит/с	10 Мбит/с	100 Мбит/с
Домашняя страница Google (160 кбит/с)	00:00:05	00:00:01*	00:00:00	00:00:00
Музыка (5 Мбит/с)	00:00:36	00:00:20	00:00:04	00:00:00*
Видеоклип (20Мбит/с)	00:10:25	00:01:20	00:00:16	00:00:02
CD/ кинофильм низкого качества	06:04:35	00:46:40	00:09:20	00:00:56
DVD/ кинофильм высокого качества	34:43:20	04:26:40	00:53:20	00:05:20

* Приближенное значение

Из таблицы, например, видно, что на скачивание кинофильма качества DVD на скорости 256 кбит/с понадобится коло полутора дней, тогда при 100 Мбит/с – немногим более 5 минут.
В США до 2008 года нормой считалось 100 кбит/с . С декабря 2010 года требования к ШПД повысились и составляют в нисходящем направлении не менее 4 Мбит/с и в восходящем – 1 Мбит/с.

Исторически ШПД прошло много технологий, основные из которых подлежат рассмотрению в настоящей и последующих главах.

23.1. Сети сотовой связи стандарта GPRS и EDGE

В настоящем разделе рассмотрению подлежат пакетная радиопередача GPRS (General Packet Radio Service) и система EDGE повышенной скорости передачи данных для развития GSM (Enhanced Data Rates for GSM Evalution).

23.1.1. Сети сотовой связи стандарта GPRS

Введение передачи данных в GPRS с коммутаций пакетов КП привело к появлению сети, параллельной GSM с коммутацией каналов КК. GPRS использует много ресурсов GSM, однако основные сетевые элементы соединены друг с другом при помощи отдельной базовой сети, в основе которой лежит протокол IP. Используются все основные компоненты сети GSM, но для поддержки пакетной передачи данных, в GPRS добавляются два новых компонента: 1) SGSN – коммутатор пакетов ядра сети GPRS (Serving GPRS Support Node), работает таким же образом, как и MSC в GSM. SGSN определяет маршрут передаваемых пакетов и пересылает их на соответствующие узлы. 2) GGSN – шлюз ядра сети GPRS (Gateway GPRS Support Node), обеспечивает интерфейс между базовой сетью GPRS и внешними сетями передачи данных (Интернет). На рис. 23.1 приведена архитектура GPRS.

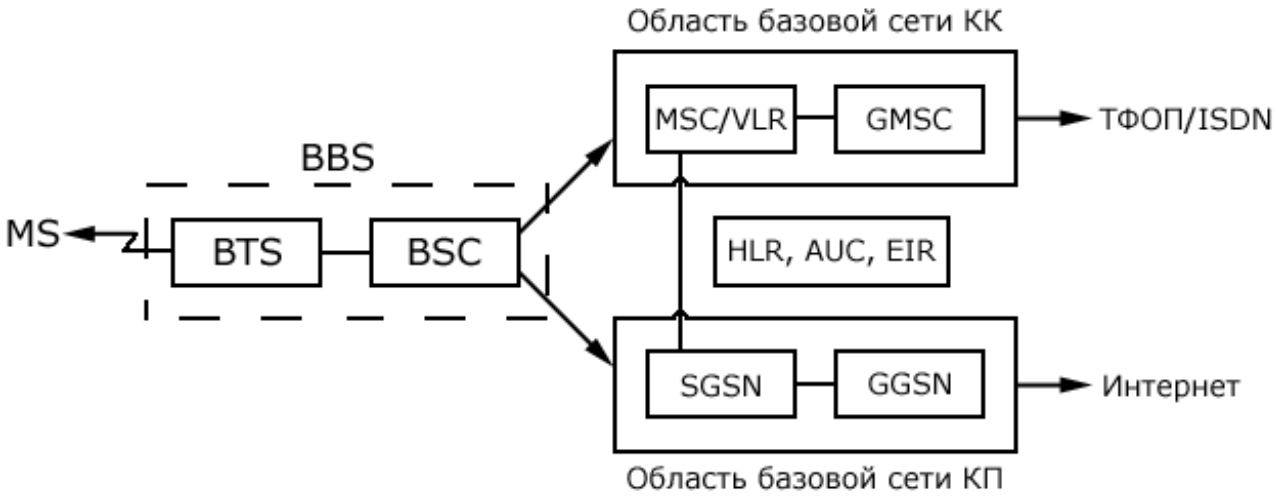


Рис. 23.1. Архитектура GPRS

Физический уровень системы GPRS очень похож на физический уровень стандартной системы GSM. Тем не менее, пакетная передача и асимметрия трафика потребовали внесения

в него следующих изменений:

- многослотовый режим, в котором одной подвижной станции может быть выделено до восьми временных слотов в кадре;
- асимметричность пакетного трафика, при котором нисходящему и восходящему трафику выделяются разные ресурсы.

В GPRS используется двухуровневое канальное кодирование: блочное и сверточное. В таблице 23.1 приведены скорость кодирования и скорости передачи для различных схем кодирования. Под скоростью кодирования понимается отношение длины блока до кодера данных к длине блока после кодера. Скорость передачи приведена для одного слота кадра. Схемы кодирования соответствуют различным условиям состояния радиоканала и требованиям к услуге.

Таблица 23.1. Скорость кодирования и скорость передачи для схем кодирования GPRS

Схема кодирования	Скорость кодирования	Скорость передачи Кбит/с
CS-1	1/2	9,05
CS-2	2/3	13,04
CS-3	3/4	15,06
CS-4	1	21,4

Скорость кодирования CS-1 используется при плохих радиоканалах, а CS-4 при очень хороших. В CS-4 кодирование не используется и скорость передачи возрастает до 21,4 Кбит/с на один слот, что позволяет достигнуть скорости 171,2 Кбит/с при выделении одному пользователю всех восьми слотов.

23.1.1.1. Информационная безопасность GPRS

Технология информационной безопасности GPRS, хотя и основана на тех же принципах, что и GSM, имеются, однако некоторые специфические угрозы. К ним относятся угрозы со стороны сети общего пользования Интернет. Операторы должны принять дополнительные меры для защиты соединения между шлюзом GGSN и Интернет. GPRS подвержена некоторым из угроз, с которыми сталкивается проводная Интернет-технология. Следует также отметить, что пересылка GPRS-пакетов параллельно в нескольких временных слотах,

снижает риск подслушивания зашифрованных данных. Это означает, что даже, если злоумышленник проникнет на базовую станцию, он не сможет легко расшифровать GPRS-трафик.

23.1.2. Сети сотовой связи стандарта EDGE и показатели скорости передачи

Технология повышенной скорости передачи данных для EDGE позволяет удовлетворить потребность в более высоких скоростях, чем GPRS в одном временном слоте. Для этого в EDGE использованы следующие усовершенствования для GSM. Первое усовершенствование- это применение восьмибитовой фазовой модуляции 8-PSK (8-Phase Shift Keying) в высокоскоростных режимах. В низкоскоростных режимах по-прежнему используется GMSK- модуляции, как и в GSM. При 8-PSK, каждый информационный символ представляется тремя битами, что позволяет увеличить в три раза скорость передачи данных по сравнению со стандартной системой GSM. Другая особенность системы EDGE- это медленный перескок частоты, которая в GSM является необязательной. Скачкообразную перестройку частоты можно рассматривать как изменение частоты, помогающее снизить замирание из-за многолучевого распространения. При использовании перескока частоты каждый кадр передается на четырех различных несущих. Если на какой-то частоте имело место замирание, то при изменении частоты на 200…400 кГц, замирания с большой вероятностью не будет. При этом снижается вероятность длительных замираний, и в сочетании с перемежением, снижается вероятность групповых ошибок, а с одиночными производится исправление с помощью кодера канала. Следующее важное свойство системы EDGE - контроль качества радиоканала. Подвижные станции передают на базовые станции информацию о качестве канала. На основании этого принимается решение о том, какую комбинацию модуляции и схемы кодирования MCS (Modulation and Coding Scheme) следует использовать. В системе EDGE могут применяться два типа модуляции (8-PSK и GMSK) и девять скоростей кодирования. В таблице 23.2 приведены скорость кодирования и скорости передачи для схем кодирования EDGE.

Таблица 23.2. Скорость кодирования и скорость передачи для схем кодирования EDGE

Схема кодирования	Модуляция	Скорость кодирования	Скорость передачи Кбит/с

MCS-9	8-PSK	1,0	59,2
MCS-8	8-PSK	0,92	54,4
MCS-7	8-PSK	0,76	44,8
MCS-6	8-PSK	0,49	29,6
MCS-5	8-PSK	0,37	22,4
MCS-4	GMSK	1,0	17,6
MCS-3	GMSK	0,8	14,8
MCS-2	GMSK	0,66	11,2
MCS-1	GMSK	0,53	8,8

Анализ таблицы подтверждает, что технология EDGE позволяет повышать скорость передачи данных. Минимальная скорость EDGE для схемы кодирования MCS-5 скорость передачи 22,4 Кбит/с выше максимальной скорости GPRS для схемы CS-4 без использования кодирования – 21,4 Кбит/с.

Дальнейшее развитие стандарта GSM пошло по пути интеграции технологии EDGE в новую систему радиодоступа GERAN (GSM/EDGE Radio Access Network), рассматриваемую как альтернативное совершенствование на пути к системе мобильной сети третьего поколения.

23.1.2.1. Метод перескока частоты

Для повышения устойчивости к узкополосным помехам в EDGE используется расширение спектра методом перескока частоты FHSS (Frequency Hopping Spread Spectrum). При этом доступная полоса частот разбивается на много каналов с меньшими полосами, разделенными защитными интервалами. Передатчик и приёмник используют один из этих каналов на

протяжении некоторого времени, а затем производится перескок на другой канал. Схема использования отдельных каналов называется последовательностью перескоков. Время, на протяжении которого используется канал с определенной частотой, называется временем пребывания.

На рис. 23.2 приведён пример системы FHSS, на котором показано пять бит полезных данных, каждый продолжительностью t_b. Работая по схеме с медленным перескоком, передатчик использует частоту f_2 на протяжении времени пребывания t_d, необходимого для передачи первых трех битов. Затем передатчик перескакивает на следующую частоту f_3.

На рис. 23.3 и 23.4 приведены упрощенные структурные схемы передатчиков и приемников, работающие по технологии FHSS. На первом этапе передатчик схемы FHSS осуществляет модуляцию передаваемых данных согласно одной из схем цифро-аналоговой модуляции. В качестве примера можно взять схему частотной модуляции FSK (Frequency Shift Keying).

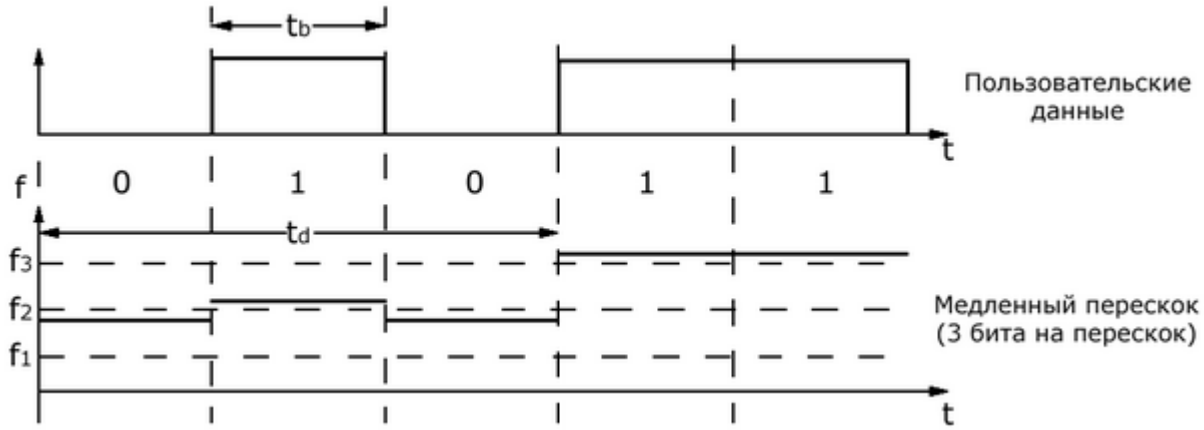


Рис. 23.2. Система FHSS

модуляции). Пусть по схеме FSK для двоичного нуля используется частота f_0, а для двоичной единицы - частота f_1. В результате формируется узкополосный модулирующий сигнал. На следующем этапе выполняется перескок частоты в соответствии с установленной последовательностью перескоков. Сведения о последовательности перескоков направляются в синтезатор частот, генерирующий несущие частоты f_i. При второй модуляции модулирующий узкополосный сигнал накладывается на несущую частоту и формируется новый расширенный сигнал. При этом нулю соответствует частота $f_i + f_0$, а единице – частота f_i+f_1. Если различные передатчики схемы FHSS используют только неперекрывающиеся

последовательности перескоков, т.е. никогда не работают на одинаковой частоте в одно и то же время, то их передачи не мешают друг другу. Такой подход требует координации работы всех передатчиков и согласования их последовательностей перескоков.

Рис. 23.3. Схема устройства передатчика, работающего по технологии FHSS

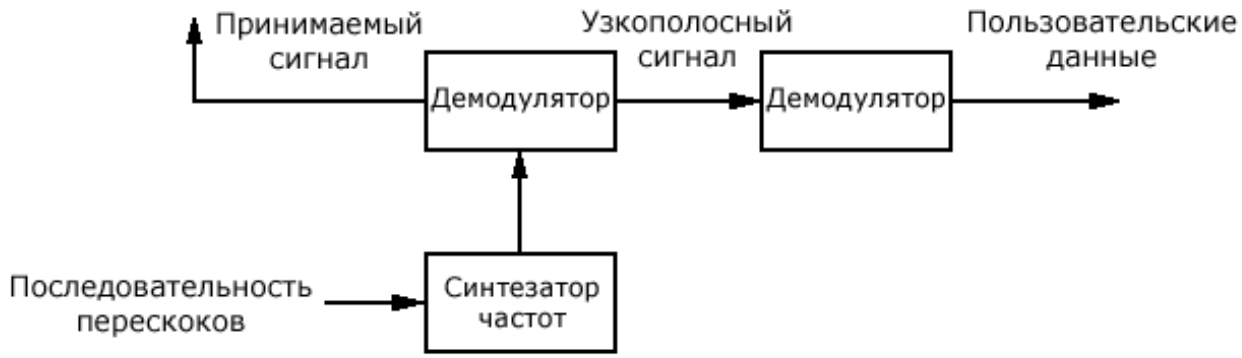


Рис. 23.4. Схема устройства приёмника, работающего по технологии FHSS

Приемник системы FHSS должен знать используемую последовательность перескоков. Кроме того, он должен постоянно поддерживать синхронизацию с передатчиком. При приеме выполняются действия, обратные процедуре модуляции, в результате чего передаваемые данные восстанавливаются. Кроме того, необходимо использовать несколько фильтров (на упрощенной диаграмме рис. 23.4 они не показаны).

23.2. Сети сотовой связи стандарта UMTS

23.2.1. Принцип работы системы CDMA

В отличие от GSM, основанных на множественном доступе FDMA и TDMA, в основу стандартов сотовых сетей связи третьего поколения 3G положен множественный доступ с кодовым разделением каналов CDMA. Рассмотрим принцип действия CDMA. К каждому

пакету данных перед его передачей добавляется уникальный код. Такой код используется на приемном конце для восстановления. Таким образом, CDMA дает возможность использовать одновременно одну и ту же частоту для разных соединений. Эти коды используются для разделения различных пользователей в кодовом пространстве. Главная задача найти «хорошие» коды и отделить нужный сигнал от шума, создаваемого окружением и сигналами между другими пользователями. В CDMA каждый битовый интервал разбивается на m периодов, называемых чипами (кодовыми последовательностями). Обычно битовый сигнал заменяется чиповой последовательностью из 64 или 128 бит. Чтобы передать бит, равный 1, станция посылает свою чиповую последовательность. Чтобы передать бит, равный 0, станция передает дополнение этой чиповой последовательности (т.е. все единицы меняются на нули, а нули -на единицы). Никаких других комбинаций передавать определенной станции не разрешается. Например, если передатчику А присвоена чиповая последовательность 010011, то передача бит со значением «1» передается кодом 010011, а бит со значением «0» - кодом 101100.

Таким образом, CDMA является одной из форм расширения спектра. В отличие от GSM, где расширение спектра осуществляется методом перескока частоты, в CDMA расширение спектра осуществляется методом прямой последовательности DSSS (Direct Sequence Spread Spectrum). В CDMA расширение спектра служит для увеличения эффективной пропускной способности. Если имеется полоса шириной 1МГц, на которой работают 100 пользователей, то все пользователи используют всю ширину диапазона (1МГц) так, что чиповая скорость составляет 1Мчип/с.

Чипы пользователей подбираются таким образом, чтобы попарно были ортогональны, т.е. скалярное произведение двух чипов равно 0. Генерирование таких чиповых последовательностей осуществляется с помощью метода, известного как коды Уолша. Векторы (3,-2,4) и (-2,3,3) являются ортогональными: (3,-2,-4)* (-2,3,3) = -6-6+12=0. Однако векторы (1,2,3) и (4,2,-6)- неортогональны друг к другу (скалярное произведение равно -10), а векторы (1,2,3) и (4,2,-3) «почти» ортогональны (скалярное произведение равно -1), т.е. близко к нулю. Другим требованием к выбору чиповой последовательности является обладание хорошей автокоррекцией.

Объясним, что подразумевается под хорошей автокоррекцией. К примеру, код Баркера (+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1) обладает хорошей автокоррекцией, т.е. его скалярный квадрат имеет большое значение, равное 11. При сдвигах кода Баркера на один или несколько чипов (представьте сдвиг 11-чипового кода Баркера относительно самого себя, повторенный

несколько раз) абсолютная величина корреляции (скалярное произведение) не превышает 1. Ее значение будет оставаться таким низким до тех пор, пока код опять точно не совместится сам с собой.

Пример сдвига кода Баркера на 4

+1	-1	+1	+1	-1	+1	+1	+1	-1	-1	-1	Код Баркера
-1	+1	+1	+1	-1	-1	-1	+1	-1	+1	+1	Сдвиг на 4
-1	-1	+1	+1	+1	-1	-1	+1	+1	-1	-1	скалярное произведение равно -1

Прежде, чем разбирать алгоритм работы, рассмотрим следующую аналогию. Представьте себе зал ожидания в аэропорту. Множества пар оживленно беседуют. Временное уплотнение можно сравнить с ситуацией, когда все люди находятся в центре зала и говорят по очереди. Частотное уплотнение мы сравним с ситуацией, при которой люди находятся в разных углах и ведут свои разговоры, которые не слышны другим. Это происходит одновременно, но независимо. Для CDMA лучше всего подходит сравнение с ситуацией, когда все в центре зала, однако каждая пара говорящих использует свой язык общения. Франкоговорящие промывают косточки всем остальным, воспринимая чужие разговоры, как шум. Таким образом, ключевой идеей CDMA является выделение полезного сигнала при игнорировании всего остального. Далее следует упрощенное описание технологии CDMA.

Основы функционирования схемы CDMA можно объяснить с помощью следующих примеров.

Двум передатчикам, A и B, необходимо передать данные. Схема CDMA присваивает им следующие ключевые последовательности: ключ Ak=010011 и ключ Bk=110101. Передатчику A нужно послать бит Ad = 1, передатчику B – бит Bd=0. В этом примере удобно кодировать бинарный ноль как -1, а бинарную единицу как +1. В результате Ad =+1, Bd=-1. Тогда к ним можно применять обычные правила сложения и умножения. Оба передатчика расширяют свой сигнал, используя ключи в качестве чиповых последовательностей (здесь термин «расширение» означает обычное умножение бита данных на всю чиповую последовательность). В действительности для расширения к отдельным битам данных применяются части намного большей чиповой последовательности.

Убедимся, что оба чипа ортогональные.

Ак	-1	+1	-1	-1	+1	+1	
Вк	1	+1	-1	+1	-1	+1	
Ак*Вк	-1	+1	+1	-1	-1	+1	0

Как видно, скалярное произведение Ak и Bk равно нулю. Передатчик А посылает сигнал As =Ad *Ak = +1 * (-1, +1, -1, -1, +1,+1) =(-1,+1, -1, -1, +1, +1). Передатчик В для расширения своего сигнала производит те же действия, но со своим кодом: Bs = Bd * Bk = -1 * (+1, +1, -1, +1, -1, +1) = (-1, -1, +1, -1, +1, -1).

Затем оба сигнала одновременно передаются на одинаковой частоте, поэтому в пространстве они накладываются друг на друга. Если интенсивность сигналов при приеме одинакова, а влиянием остальных передатчиков и шумом окружающей среды можно пренебречь, то приемник получит следующий сигнал C=As + Bs =(-2, 0, 0, -2, +2, 0). Допустим приемнику необходимы данные передатчика А и он настраивается на код А. Иначе говоря, для сужения применяется код передатчика А: C*Ак = (-2, 0, 0, -2, +2, 0) * (-1, +1, -1, ¬1, +1, +1) = 2 + 0 +0 + 2 + 2 + 0 = 6. Поскольку рузультат намного превышает 0, приемник детектирует бинарную единицу. При настройке на передатчик В, т.е. при использовании кода В приемник получит сигнал C*Вк = (-2, 0, 0, -2, +2, 0) * (+1, +1, -1, +1, -1, +1,) = - 2 + 0 + 0 – 2 – 2 + 0 = - 6. Результат отрицательный, поэтому детектируется бинарный ноль.

В этом примере было сделано несколько упрощений. Коды были очень простыми, но, по крайней мере, ортогональными. Что более важно, шумы считались пренебрежительно малыми, хотя в действительности шумы могут существенно влиять на передаваемый сигнал С. Соответственно, полученные результаты (+6, -6) могут оказаться не столь хорошими, а, например, близкими к нулю. В этом случае решить, что представляет собой сигнал – 0 или 1, - будет намного сложнее. Кроме того, интенсивность обоих принимаемых сигналов полагалась одинаковой. Однако, что произойдет, если интенсивность одного сигнала будет намного больше другого? Пусть, например, интенсивность сигнала в пять раз больше чем интенсивность сигнала А. Тогда C = As + 5*B = (-1, +1, -1, -1, +1, +1) + (-5, -5, +5, -5, +5, -5) = (- 6, - 4, + 4, - 6, + 6, -4). Допустим, что приемнику нужно получить данные передатчика В: C*Вк = - 6 – 4 – 4 -6 - 6 – 4 = -30. Бинарный ноль, посланный передатчиком В, легко детектируется. При приеме данных передатчика А сигнал будет выглядеть так: C*Ак = – 6 – 4 – 4 + 6 + 6 – 4 = 6. Понятно, что по абсолютной величине более сильный сигнал превосходит более слабый (+30 и +6). В то время как – 30 детектируется как бинарный ноль, для +6 принять решение не так легко: в сравнении с -30 значение +6 находится близко к нулю и

поэтому может интерпретироваться как шум. Вспомним пример: если кто-то разговаривает на своем языке слишком громко, то использовать другой язык в качестве ортогонального кода бессмысленно – все равно вас никто не поймет, а слова лишь увеличат шум. При всей своей крайней упрощенности описанный пример указывает на то, что в системах CDMA необходим контроль мощности передачи. Это одна из крупнейших проблем, возникающих при использовании систем CDMA.

Уровни мощности, воспринимаемые приемником, зависят от того, насколько далеко находятся базовые станции. Уровни мощности контролируются базовыми станциями, выдающими сигнал увеличить или уменьшить.

23.2.2. Сравнение систем TDMA/FDMA и CDMA

Сравнение систем TDMA/FDMA и CDMA проведем в порядке перечисления преимуществ и недостатков первых, а затем вторых [79]. Преимущества систем TDMA/FDMA:

- самая распространенная технология беспроводных сотовых сетей в мире;
- более дешевая сеть;
- международный роуминг. Глобальное присутствие GSM позволяет абонентам использовать свой телефон по всему миру.

Недостатки систем TDMA/FDMA:

- жесткий роуминг. TDMA/FDMA использует «жесткий» перевод пользователя из одной соты в другую. Для каждого пользователя выделен специальный временной слот, но, когда абонент переходит в другую соту, может случиться так, что пользователю просто некуда будет присоединиться (при отсутствии свободного слота);
- искажения. Отношение «сигнал/шум» меньше и, поэтому вероятность искажения сигнала больше.

Преимущества CDMA:

- эффективное использование полосы, что дает дополнительную емкость и более высокую пропускную способность. В широко распространенной реализации системы CDMA IS-95 скорость передачи данных 115,2 кбит/с может быть достигнута без внесения изменений на физическом уровне;
- мягкий роуминг. Мобильная станция может плавно переключаться между двумя сотами. Это достигается с помощью установки соединения с двумя базовыми станциями одновременно. В CDMA это реализуется с использованием одинаковых кодов, что приводит к меньшему числу отказов, чем в сетях TDMA/FDMA;

- меньшее искажение. У CDMA отношение «сигнал/шум» больше, что обеспечивает более высокое качество связи.

Недостатки CDMA:

- дороговизна;
- отсутствие международного роуминга. Из-за ограниченного распространения CDMA по миру, эти сети не могут обеспечить международный роуминг;
- планирование размеров ячеек в системах CDMA сложнее, чем в более жестких системах TDMA/FDMA. При добавлении нового пользователя в ячейку CDMA ячейка уменьшается, в ней повышается уровень шума.

23.2.3. Сети сотовой связи стандарта UMTS

Международным союзом электросвязи была разработана концепция развития мобильных сетей связи третьего поколения 3G под названием IMT-2000, задачей которой было достичь более высоких скоростей передачи данных в сравнении с сетями поколений 2 и 2,5. При этом основные требования по минимальной пропускной способности были сформулированы не менее:

- 2 Мбит/с внутри помещений и для терминалов, перемещающихся с пешеходной скоростью;
- 384 кбит/с для терминалов, перемещающихся со скоростью не более 120 км/ч в областях городской застройки;
- 144 кбит/с в сельской местности и для быстро перемещающихся транспортных средств.

Было предложено несколько стандартов IMT - 2000, одним из которых является европейский и называется универсальная система мобильной связи UMTS (Universal Mobile Telecommunication System). Эта концепция содержит также следующие требования:

- Все технические характеристики системы должны быть точно определены (как в системе GSM), а основные интерфейсы должны быть стандартизованными и открытыми. При этом разработанные технические требования должны выполнятся во всем мире.
- По сравнению с GSM система 3G должна выйти на совершенно новый уровень, причем во всех аспектах. Однако на начальном этапе такая система должна быть совместимой, по крайней мере, с GSM и ISDN.

- Система 3G должна поддерживать мультимедийную среду со всеми ее компонентами.
- Система 3G должна обеспечивать широкополосный радиодоступ с тем, чтобы стать пригодной во всем мире. Термин «широкополосный» используется, чтобы отразить промежуточные требования к пропускной способности систем 3G, между узкополосными системами 2G и средствами фиксированной, проводной, связи.
- Услуги, предоставляемые конечному пользователю, не должны зависеть от особенностей используемых технологий радиодоступа, а сетевая инфраструктура не должна ограничивать появление новых услуг. Другими словами, речь идет о полном разделении технологической базы и услуг, использующих эту базу.

В основу UMTS положена технология широкополосного доступа с кодовым разделением WCDMA. По сравнению с другими стандартами CDMA принятый в UMTS стандарт более устойчив и хорошо помехозащищён, надёжен в отношении перехвата. Для реализации этих преимуществ WCDMA занимает более широкую полосу частот - 5 МГц.

Для разработки стандартов систем 3G было проведено объединение шести организаций, одной из которых ETSI. Это объединение, занимающееся стандартизацией, получило название 3GPP (Third Generation Partnership Project, партнерство в области технологий 3G). Идентификатор документов3GPP начинается с префикса 3GPP, за которым следуют две буквы: TS (Technical Specification) для технических спецификаций или TR (Technical Reports) для технических отчетов.

Спецификациями на UMTS в развитие последовательно разрабатывались предусмотрено следующие версии (release) -R99, R4, R5, R6, R7. Версия R99 основана на принципах GPRS и включает две наземные сети доступа и две области базовой сети (с коммутацией каналов КК и коммутацией пакетов КП). На рис. 23.5 приведена структура сети UMTS версии R99. UMTS версии R99 совместима с сетью GSM на уровне базовой сети. Область наземного радиодоступа BSS и базовая сеть КК практически такая же, как и в GSM. Область базовой сети КП - это по существу усовершенствованная система GPRS.

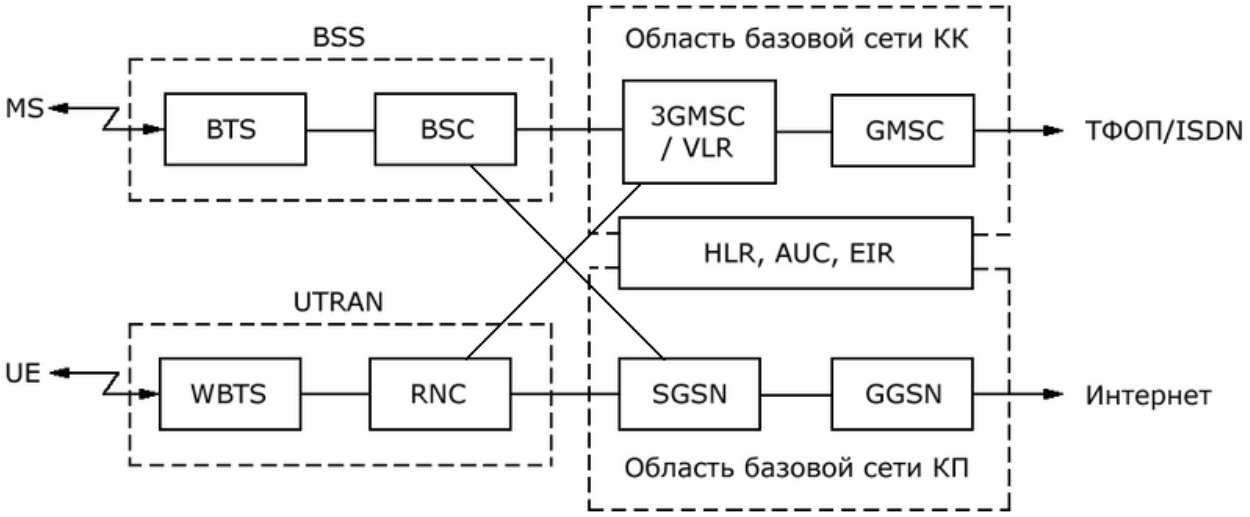


Рис. 23.5. Структура сети UMTS версии R99

Основное отличие от GSM состоит в том, что в сети радиодоступа UMTS используется технология широкополосного множественного доступа с кодовым разделением каналов WCDMA (Wideband Code Division Multiple Access). Когда говорят конкретно о системе UMTS с технологией WCDMA, используют для обозначения области радиодоступа терминологию UTRAN (Universal Terrestrial Radio Access Network, универсальная наземная сеть радиодоступа). Как видно из рис. 23.5 UTRAN включает широкополосную базовую станцию WBTS (Wide Base Transceiver Station) и контроллер радиосети RNC (Radio Network Controller). Оконечное оборудование в сети UMTS называется оборудованием пользователя UE (User Equipment). UE, как и MS в сети GSM, состоит из мобильного абонентского устройства ME (Mobile Equipment) и модуля идентификации абонента USIM (UMTS Subscriber Identity Module) - чипа, аналогичного SIM-карте в GSM. Базовая станция UMTS называется узлом B (Node B). Каждый Node B подсоединен к одному контроллеру радиосети RNC (Radio Network Controller). Контроллер RNC управляет ресурсами подсоединенных к нему узлов B (базовых станций) и является аналогом контроллера BSC в сети GSM. Область базовой сети КК способна поддерживать как абонентов сети GSM (MS), так и абонентов UE. Это приводит к изменению в оборудовании MSC (в UMTS оно называется 3GMSC), HLR, VLR, AUC, EIR. Механизм обеспечения информационной безопасности по-разному устанавливается в сети 2G и 3G. Поэтому область базовой сети КК должна поддерживать оба эти механизма.

Разработка R99 на систему UMTS проходила в то время, когда технология, основанная на IP-протоколе, стала использоваться для передачи не только данных, но и речи, видео. Передача речевых услуг поверх IP-протокола в обычных фиксированных сетях связи явилось причиной

создания и развития мультисервисных сетей связи. Поэтому целью последовавших за R99 версий UMTS была ее полная интеграция в сеть IP с одновременным сосуществованием двух различных сетей, построенных на базовой сети с коммутацией каналов и базовой сети с коммутацией пакетов. Версия R99 обеспечивала скорость передачи до 384 Кбит/с.

Версия R4. Определены изменения в базовой сети с коммутацией каналов, при которых новые функциональные возможности не добавляются. Введены понятия медиашлюза MGW, сервера MSC и шлюза сигнализации SGW, что позволило логически разделять пользовательские данные и информацию сигнализации в центре коммутации подвижной связи MSC. Введены усовершенствования, обеспечивающие повышение скорости передачи для подвижных пользователей.

Версия R5 предусматривает полный переход к коммутацией пакетов, ввод новой модели вызова, домашний регистр HLR заменяется/дополняется сервером HSS домашней сети. С точки зрения услуг главную роль в R5 и более поздних версиях будет играть мультимедийная система IMS (IP Multimedia Subsystem). IMS представляет собой отдельное системное решение, способное использовать различные сети, одна из которых и есть UMTS. IMS позволяет абоненту использовать сложные услуги по передаче сообщений и мультимедиа. Технология IMS обеспечивает предоставление мультимедийных услуг через сеть IP. Она позволяет однократно реализовать общую базовую функциональность и затем использовать ее всем приложениям IMS. Общая функциональность включает создание услуг, взаимодействие с подсистемой обеспечения качества обслуживания и др. IMS рассматривается как один из базовых элементов, определяющих будущее развитие телекоммуникаций. Европейский институт стандартизации в области злектросвязи ETSI одобрил IMS в качестве основы сетевой инфраструктуры сетей следующего поколения NGN (Next Genereration Networks) [80]. Среди основных свойств архитектуры IMS можно выделить следующие:

- многоуровневость - разделяет уровни транспорта, управления и приложений;
- независимость от среды доступа — позволяет операторам и сервис-провайдерам конвергировать фиксированные и мобильные сети;
- полная интеграция мультимедийных приложений реального и нереального времени;
- наличие разнообразных интерфейсов, с помощью которых услуги можно адаптировать вне зависимости от типа сети и организации роуминга;
- наличие элемента IMS базы данных абонентов HSS (Home Subscriber Server), где

содержится вся информация об оконечном оборудовании, упрощает задачу адаптации услуг для разных абонентских устройств и предоставление унифицированных услуг. В HSS размещается база абонентов фиксированного и мобильного сектора. Сервер HSS является основным отличием архитектуры IMS от более ранних архитектур NGN. Именно он дает возможности для развертывания новых услуг на базе архитектуры IMS. В модели IMS уровень доступа может осуществлятся через различные сети: фиксированные (телефонные, xDSL, волоконно-оптические, Ethernet), мобильные (GSM/GPRS/EDGE, 3G, WiMAX и др.).

В версию R5 введена также технология высокоскоростной пакетный доступ в линию "вниз" HSDPA (High Speed Downlink Packet Access - высокоскоростной пакетный доступ в нисходящем канале). Скорость передачи данных до 14,4 Мбит/с (эта величина при благоприятных условиях, когда кодирование не используется). В реальных условиях помех каналов связи скорость значительно ниже.

В версии 6 добавлена технология высокоскрростной пакетный доступ "вверх" HSUPA (High Speed Uplinc Packet Access) — сервис в восходщем канале, увеличивающий скорость в восходящем канале до 5,76Мбит/с. Введение в коммерческую эксплуатацию HSUPA началось в 2007 году. Совместно с HSDPA эти технологии стали называться высокоскоростной пакетный доступ HSPA (High-Speed Packet Access).

Версия 7. Развитие технологии HSPA (HSPA+ или HSPA Evolution) и EDGE (EDGE Evolution). Теоретически максимальная скорость возросла до 42 Мбит/с в нисходящем и до 11 Мбит/с в восходящем каналах.

Таким образом, к настоящему времени совершенствуется система UMTS, предназначенная для предоставления мультимедийных услуг связи с возможностью передачи изображений и видеоинформации высокого качества на основе высокоскоростного радиодоступа в сетях общего пользования и корпоративных сетях.

23.3. Информационная безопасность UMTS

23.3.1. Ограничения в обеспечении ИБ GSM

Согласно документу ETSI TS 121 133 v.3.1.0 задача обеспечения информационной безопасности UMTS сформулирована следующим образом [81]:

- использовать решения по защите от угроз безопасности в сетях 2G, которые

показали свою эффективность;

- усовершенствовать ИБ с учетом недостатков, обнаруженных в сетях 2G;
- разработать новые способы обеспечения безопасности с учетом новых решений в технологии сети UMTS.

Для сети GSM характерны следующие ограничения в обеспечении информационной безопасности [82]:

- аутентификация односторонняя (предусматривает проверку подлинности только пользователя). Это является причиной отсутствия защиты, например, от атаки ложной базовой станцией BTS;
- отсутствует механизм обеспечения аутентификации сообщений, т.е. защиты целостности данных;
- большинство алгоритмов обеспечения ИБ GSM взломаны;
- фиксированные механизмы безопасности без возможности гибкой смены с целью усиления защиты;
- данные шифруются только на участке между мобильной станцией (MS) и базовой станцией (BTS). На участке между BTS и контролером базовых станций BSC эти данные передаются в открытом виде.

В UMTS эти ограничения сняты.

В настоящем разделе приводится описание процедур по защите приватности местоположения мобильной станции, взаимной аутентификации пользователя и сети, установление алгоритмов обеспечения целостности сообщений и шифрования, обеспечения шифрования [83,84]. В конце настоящего раздела приводятся три Дополнения, составленные на основании документа ETSI [85]. Дополнение 1 включает описание угроз ИБ в сети UMTS, а в Дополнении 2 приведены требования по защите от угроз в сети UMTS с помощью механизмов аутентификации. В Дополнении 3 приводится количественная оценка угроз в UMTS.

23.3.2. Классификация угроз ИБ в UMTS

Следует отметить, что в документах по информационной безопасности классификация угроз ИБ различных технологий сетей связи часто отличается. Ниже приведена классификация угроз ИБ для UMTS в соответствии с документом ETSI [85].

Несанкционированный доступ к важным данным (нарушение конфиденциальности).

1. Подслушивание (eavesdropping): нарушитель перехватывает сообщения без обнаружения.
2. Маскирование (masquerading): нарушитель обманывает санкционированного пользователя, представляясь законной системой, для того, чтобы получить от пользователя конфиденциальную информацию; или нарушитель обманывает законную систему, представляясь санкционированным пользователем, для того, чтобы получить услуги системы или конфиденциальную информацию.
3. Анализ трафика (traffic analysis): нарушитель наблюдает за такими данными как время, объем сообщений, источник и получатель сообщений для того, чтобы определить месторасположение пользователя или узнать важную информацию (по бизнесу и др.).
4. Просмотр (browsing): нарушитель просматривает хранимые данные в поиске важной информации.
5. Утечка (leakage): нарушитель получает важную информацию, используя законный доступ к данным.
6. Интерференция (interference): нарушитель наблюдает реакцию системы, отправляя в нее запросы. Например, нарушитель может инициировать соединение и затем наблюдать на радио-интерфейсе за такими данными, как источник и получатель сообщений, объем сообщений.

Несанкционированная манипуляция важными данными (нарушение целостности).

Манипуляция сообщениями (manipulation of messages): сообщение может умышленно изменено, вставлено, повторено или уничтожено нарушителем.

Нарушение работы сети (приводящее к отказу в обслуживании или снижению готовности).

- Вмешательство (intervention): нарушитель может препятствовать обслуживанию санкционированного пользователя с помощью преднамеренных помех его трафику, сигнализации или данным управления.
- Уменьшение ресурсов (resource exhaustion): нарушитель может препятствовать обслуживанию санкционированного пользователя в результате создания перегрузки.
- Неправильное использование приоритетов (misuse of privileges): пользователь или обслуживающая сеть используют свои приоритеты для получения несанкционированного обслуживания или информации.
- Злоупотребление услугами (abuse of services): нарушитель может злоупотреблять некоторыми специальными услугами или средствами для того, чтобы получить

преимущества или вызвать нарушения в работе сети.

Отказуемость (repudiation): пользователь или сеть отказываются от действий, которые имели место.

Несанкционированный доступ к обслуживанию (unauthorized access to services).

1. Нарушитель может получить доступ к обслуживанию, маскируясь под пользователя или объекта сети.
2. Пользователь или объект сети может получить несанкционированный доступ к обслуживанию, не используя их права доступа.

23.3.3. Обеспечение защиты приватности местоположения мобильной станции

Область базовой сети коммутации каналов сохраняется и в последующих версиях UMTS после R99, обеспечивая их совместимость с прежними мобильными системами связи. В UMTS так же, как и в GSM для защиты приватности местоположения и обеспечения конфиденциальности идентификатора пользователя IMSI в области базовой сети КК применяется временной идентификатор TMSI. Подобные временные идентификаторы применяются и в области базовой сети КП. Для того чтобы отличить их от TMSI здесь используется термин «временной идентификатор мобильного абонента при пакетной коммутации» P-TMSI (Packet Temporary Mobile Subscriber Identity). При установленном соединении периодически производится смена временных идентификаторов TMSI/P-TMSI. Случай, когда нельзя использовать временные идентификаторы, - это первоначальная регистрация, поскольку в этот момент сеть еще не знает постоянного идентификатора IMSI. Предположим, что пользователь уже идентифицирован в обслуживающей сети SN (Serving Network) по номеру IMSI. Затем SN (VLR или SGSN) присваивает данному абоненту TMSI/P-TMSI и поддерживает соответствие между временным идентификатором и IMSI. Каждый VLR или SGSN следит за тем, чтобы не присвоить одно и то же значение TMSI/P-TMSI одновременно двум разным пользователям. TMSI/P-TMSI передается пользователю в зашифрованном виде. Затем этот идентификатор используется при сигнализации, пока сеть не присвоит новое значение TMSI/P-TMSI.

Поскольку временной идентификатор носит локальный характер, то, как и в GSM, он должен сопровождается идентификатором области местоположения. Поэтому к TMSI добавляется идентификатор области местоположения LAI (Local Area Identity), а к P-TMSI - идентификатор области маршрутизации RAI (Routing Area Identity). Каждая область местоположения LA (Local Area) однозначно определяется идентификатором LAI,

состоящим:

LAI = MCC + MNC + код LA, где MCC -мобильный код страны (три цифры);

MNC - мобильный код сети (2-3 цифры);

LA - номер, идентифицирующий данную область.

Область базовой сети КП имеет свою процедуру регистрации местоположения, в основе которой лежит понятие области маршрутизации RA (Routing Area). Область RA определяется по аналогии с областью LA (т.е. как зона, в пределах которой оборудование пользователя UE может перемещаться без процедуры обновления области маршрутизации). В то же время область RA -это «подмножество» области LA: одна область LA может включать несколько областей RA, но не наоборот.

Когда оборудование пользователя (MS и UE) переходит в новую зону, то из старой зоны (если ее адрес известен новой зоне через LAI или RAI) восстанавливается связь между IMSI и временным идентификатором TMSI/P-TMSI. Если адрес неизвестен или соединение со старой зоной не может быть установлено, то номер IMSI должен запрашиваться из оборудования пользователя.

23.3.4. Взаимная аутентификация пользователи и сети

UMTS обеспечивает взаимную аутентификацию пользователя и сети. На рис. 23.6 приведена схема взаимной аутентификации. Структура сети 3G может быть интегрирована в систему со многими различными технологиями наземного радиодоступа, что в свою очередь требует аутентификацию сети (т.е. радиодоступа). В основе механизма аутентификации лежит мастер-ключ (главный ключ) К, используемый совместно абонентским модулем USIM и базой данных домашней сети. Этот ключ длиной 128 бит никогда не становится видимым между двумя точками сети.

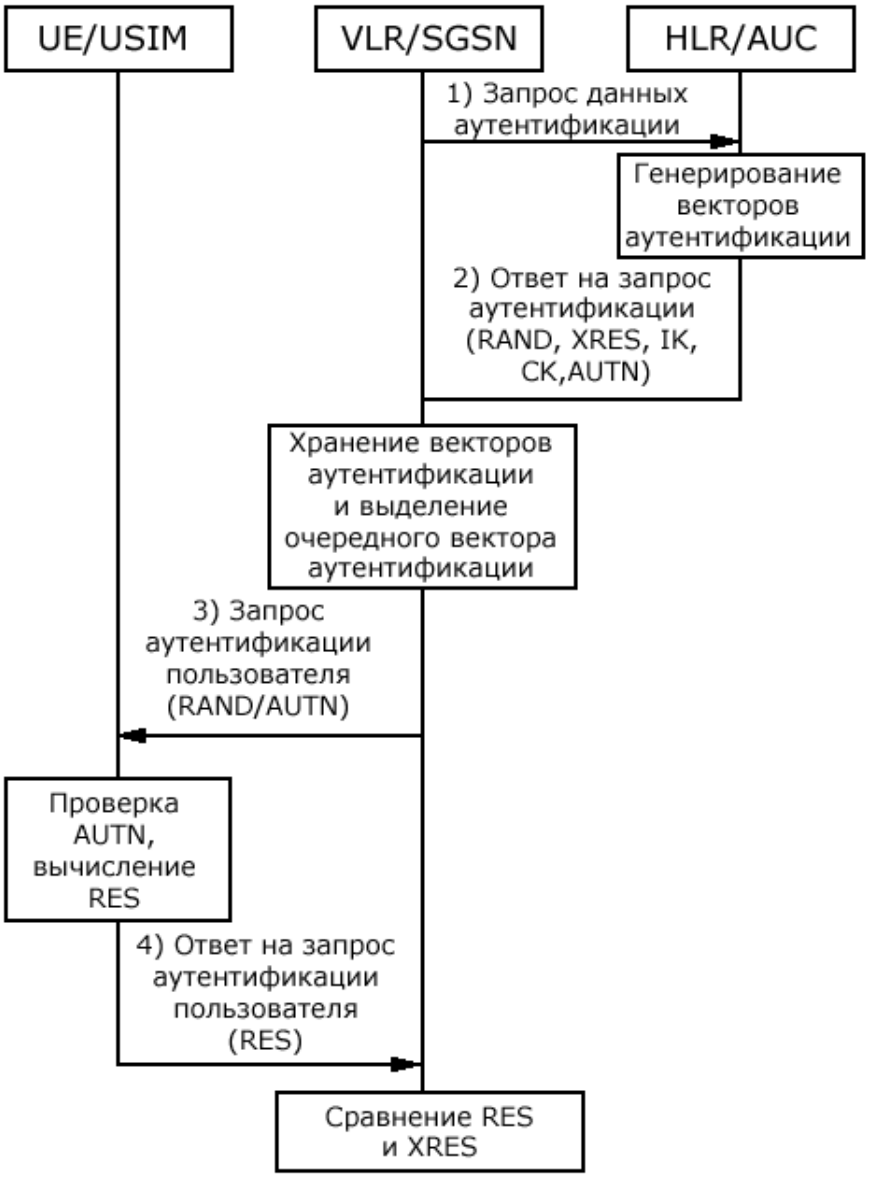


Рис. 23.6. Взаимная аутентификация

Одновременно с взаимной аутентификацией создаются ключи для шифрования и проверки целостности. При этом выполняется основной принцип криптографии (принцип Кирхгофа) в ограничении длительности использования постоянного ключа до минимума и использовании временных ключей.

Процедура аутентификации начинается после того, как пользователь будет идентифицирован в обслуживающей сети процедурой обеспечения приватности местоположения мобильной станции. Идентификация пользователя осуществляется в результате передачи в VLR или SGSN сигнальных сообщений, содержащих TMSI или P-TMSI (в исключительных случаях IMSI).

В сообщении 1 VLR или SGSN посылают в центр аутентификации AUC запрос данных об

аутентификации пользователя. В это сообщение входит идентификатор пользователя IMSI. На основе ключа К центр аутентификации AUC генерирует и передает в HLR векторы аутентификации для пользователя с идентификатором IMSI.

Каждый вектор аутентификации содержит:

- случайное число RAND (оклик);
- ожидаемый отзыв на оклик, XRES;
- ключ шифрования, СК (Cipher Key);
- ключ целостности, IK (Integrity Key);
- параметр (метка) аутентификации сети AUTN (An Authentication Token).

Процесс генерирования включает выполнение нескольких алгоритмов, которые подлежат описанию ниже в настоящем разделе. В сообщении 2 (ответ на запрос данных аутентификации) HLR передает вектор аутентификации обратно в VLR или SGSN.

Обмен сообщениями 1 и 2 производится по протоколу мобильных приложений ОКС№7 MAP. В сообщении 3 (запрос аутентификации пользователя) содержатся два параметра из вектора аутентификации - RAND и AUTN. Это сообщение 3 передается на модуль идентификации абонента USIM, который находится в защищенной от несанкционированного доступа среде (т.е. на смарт-карту UMTS - UICC, UMTS Integrate Circuit Card). Пользователь USIM использует значение параметра AUTN для того, чтобы убедиться в подлинности подключенной сети. Пользователь USIM использует RAND для того, чтобы вычислить ответ (отзыв) RES на запрос аутентификации пользователя.

В сообщении 4 (ответ на запрос аутентификации пользователя) содержится параметр RES. Это сообщение передается из оборудования пользователя UE обратно VLR/SGSN, где RES сравнивается с ожидаемым значением XRES. При совпадении RES и XRES сеть убеждается в подлинности пользователя.

Таким образом, аутентификация пользователя в UMTS так же, как и в сети GSM, осуществляется с помощью шифрования с общим ключом по протоколу типа «оклик-отзыв» (аутентифицирующая сторона посылает аутентифицируемой стороне случайное число, которое зашифровывает его по определённому алгоритму с помощью общего ключа и возвращает результат обратно).

Прежде, чем перейти к аутентификации сети в UE/USIM покажем генерирование в HLR/AUC вектора аутентификации.

На рис. 23.7 приведена схема генерирования вектора аутентификации в HLR/AUC. Центр

аутентификации содержит мастер-ключи пользователей и на основе международного идентификатора мобильной станции IMSI генерирует для пользователя векторы аутентификации. Заметим, что в сети GSM такой ключ генерирует вектор аутентификации из двух параметров - отзыв и ключ шифрования. Здесь число параметров вектора аутентификации больше.

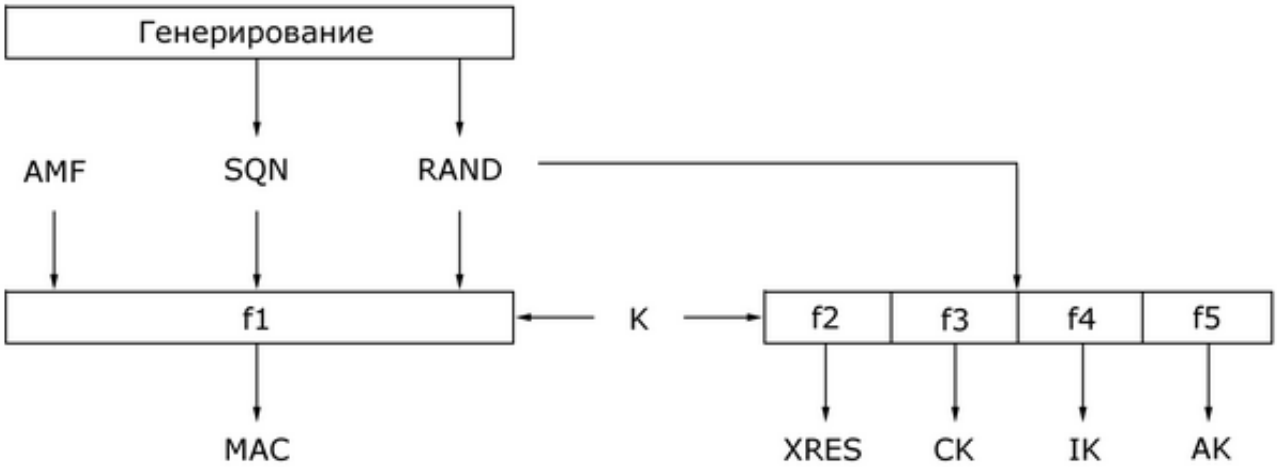


Рис. 23.7. Генерирование вектора аутентификации

Для вычисления вектора аутентификации используются пять односторонних функций – f1, f2, f3, f4, f5. Функции f1 и f5 используются для аутентификации сети, а функция f2 — для аутентификации пользователя.

Приведенные значения на рис. 23.7 означают следующее:

SQN (Sequence Number) - порядковый номер аутентификации служит для защиты от угрозы «повтор»;

AK (Anonymity Key) -ключ, используемый для шифрования SQN;

AMF (Authentication Management Field) -административное управляющее поле аутентификации. AMF может быть использовано для указания многократного шифрования;

MAC (Message Authentication Code) - код аутентичности (аутентификации) сообщения (см. приложение Г). В данном случае MAC = f(K, AMF, SQN, RAND).

В вектор аутентификации AV кроме параметра аутентификации AUTN, оклика XRES (функция f2) входят также ключ шифрования CK (функция f3) и ключ целостности IK (функция f4). Параметр аутентификации сети AUTN =SQN XOR AK || AMF|| MAC.

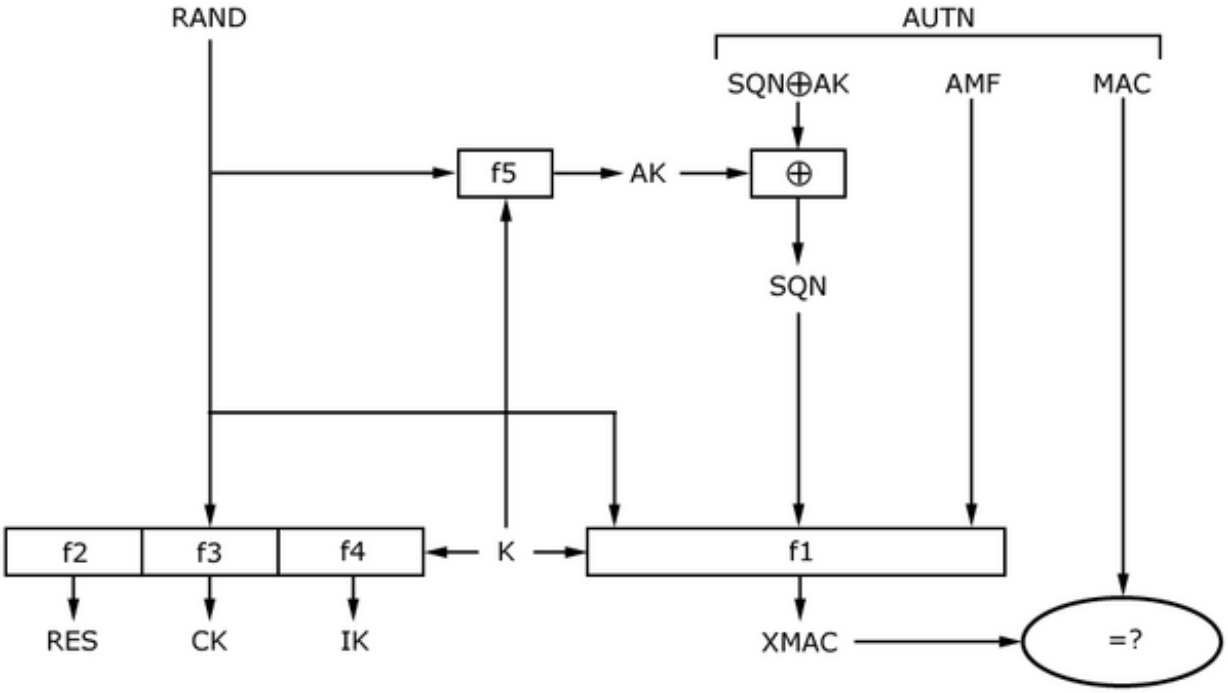


Рис. 23.8. Процедура аутентификации в UE/USIM

На рис. 23.8 приведена процедура аутентификации сети в UE/USIM. Аутентификация сети (точнее базовой станции) в UMTS основана на методе аутентичности сообщения MAC, описание которого приведено в приложении Г. Функция f5 должна быть вычислена до функции f1, поскольку f5 используется для маскировки порядкового номера SQN. Эта маскировка нужна для того, чтобы препятствовать перехвату идентификатора пользователя по SQN. Выходная функция f1, создает на стороне пользователя код аутентичности (аутентификации), обозначенный через XMAC. Она сравнивается с кодом аутентичности сообщения MAC, полученным из сети как часть параметра AUTN. Если они (MAC и XMAC) совпадают, то считается, что параметры RAND и AUTN были созданы объектом, который знает ключ K (т.е. центром аутентификации AUC домашней сети пользователя). Таким образом, пользователь убеждается в подлинности сети.

Кроме аутентификации сети на рис. 23.8 показано формирование отзыва RES для аутентификации пользователя, ключа шифрования CK и ключа целостности IK.

23.3.5. Установление алгоритмов обеспечения целостности сообщений и шифрования сообщений

Под аутентификацией сообщений понимается не только проверка подлинности источника сообщения, но и целостность данных. Проверка подлинности взаимодействующих сторон осуществляется только на момент аутентификации. Впоследствии нарушитель может начать

реализовывать атаки, передавая ложные сообщения. Примером может быть ложная базовая станция, не участвовавшая во взаимной аутентификации с оборудованием пользователя UE. После завершения взаимной аутентификации ложная базовая станция приступает к передаче ложных сообщений. Аутентификация сообщений защищает от этой угрозы ИБ с помощью механизма проверки целостности данных. Работе механизма проверки целостности отдельных сообщений UMTS предшествует процедура установления алгоритмов обеспечения целостности сообщений и шифрования сообщений (рис. 23.9).

Сообщение 1 относится к протоколу управления радио-ресурсами RRC (Radio Resource Control). Это сообщение CSC (Connection Setup Complete) сообщает контроллеру RNC завершение установления радио-соединения между UE и RNC. Сообщению 1 предшествует не показанный на рис. 23.9 обмен другими сообщениями RRC Connection Request (запрос соединения) и Connection Setup (установление соединения). Все сообщения по протоколу RRC передаются на участке UE-RNC.

Сообщение 1 содержит возможности UE по обеспечении ИБ, включая алгоритмы по обеспечению защиты целостности данных UIA (UMTS integrity algorithm) и алгоритмы шифрования UEA (UMTS encryption algorithm). В состав сообщения 1 входит также значение, называемое START и занимает поле длиной 20 бит. Это значение используется в RNC и составляет часть счетчика последовательных номеров сообщений RRC. Этот счетчик COUNT-1 предназначен для защиты от угрозы «повтор», т.е. от злоумышленного воспроизведения ранее поступивших управляющих сообщений протокола RRC (между UE и RNC). Значение START является старшими 20 битами этого счетчика и называется сверхкадром HFN (Hyper Frame Number).

Сообщение 2 - это первое сообщение сетевого уровня из нескольких управляющих сообщений по выполнению функций взаимодействия UE с областью базовой сети. Примером может быть первое из сообщений, выполняющих процедуру обновления местоположения LU (Local Update). Необходимость в этом возникает в случае, если идентификатор местоположения LAI в USIM отличается от идентификатора местоположения LAI, в котором находится UE. Затем производится описанная выше процедура взаимной аутентификации и генерации ключей.

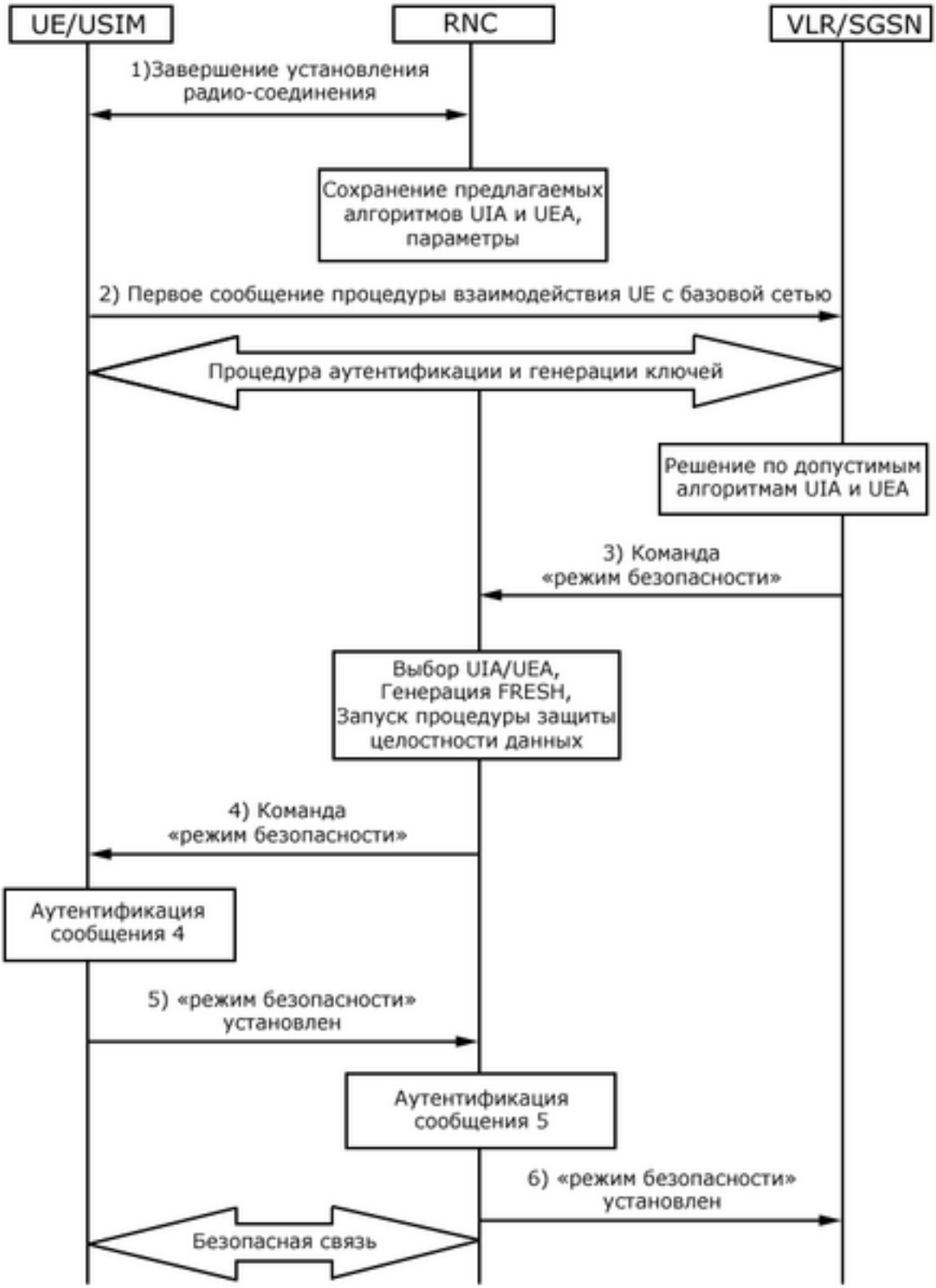


Рис. 23.9. Установление алгоритмов обеспечения целостности сообщений и шифрования сообщений

Сообщение 3 содержит алгоритмы целостности и шифрования (UIA/UEA), которые область базовой сети (VLR/SGSN) считает допустимым на участке UE-RNC. В сообщение 3 входят

также сгенерированные ключи целостности (IK) и шифрования (CK). Сообщение 3 называется командой «режима безопасности» (Security Mode Command) и расположено на прикладном уровне по протоколу RANAP (Radio Access Network Application Part) системы общеканальной сигнализации №7.

Как видно из рис. 23.9 контроллер RNC сравнивает допустимые алгоритмы UIA/UEA с возможностями UE и производит выбор. RNC производит генерацию случайного значения FRESH, используемого в алгоритме защиты целостности данных. Производится запуск процедуры защиты целостности данных.

Сообщение 4 протокола RRC (команда «режим безопасности», Security Mode Command) информирует UE о выбранных алгоритмах UIA/UEA. В сообщении 4 содержится сгенерированное в RNC случайное значение FRESH.

Механизм защиты целостности сообщений в UMTS основан на методе аутентичности сообщения MAC, описание которого приведено в приложении Г. Сообщение 4 содержит код аутентификации MAC-I (Message Authentification Code for Integrity), формирование которого приведено на рис. 23.10. Аутентификация сообщений с помощью MAC-I предусматривает использование алгоритма блочного шифрования KASUMI и общего секретного ключа целостности IK.

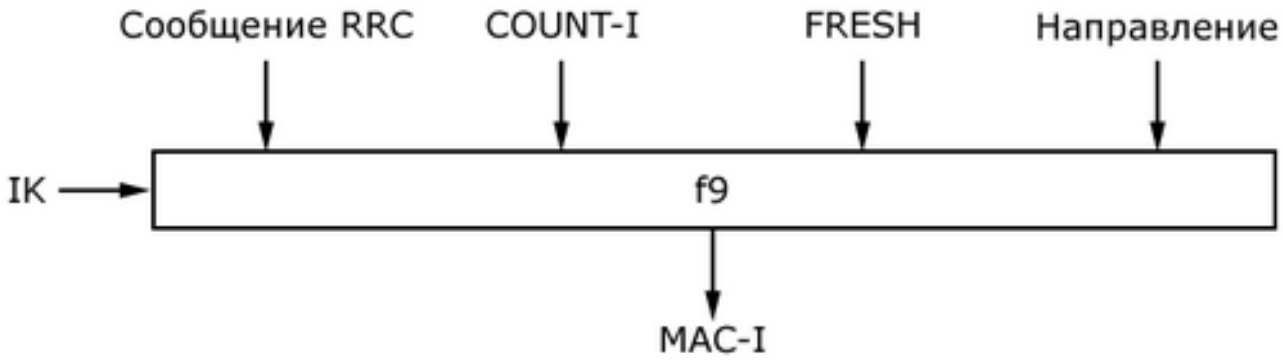


Рис. 23.10. Формирование MAC-I

Защита целостности данных реализуется на уровне управления радиоресурсами RRC, т.е. сигнальных сообщений между UE и RNC. Как видно из рисунка 10, проверке целостности подлежат сообщения RRC.

Механизм защиты выполняется формированием MAC-I с помощью односторонней функции f9, которая управляется секретным ключом IK. MAC-I представляет собой 32-битовую случайную комбинацию, которая добавляется к каждому сообщению RRC. На приемной стороне формируется XMAC-I полученного сообщения RRC, которое сравнивается с

поступившим MAC-I вместе с сообщением. Совпадение MAC-I и XMAC-I показывает, что принятое сообщение поступило от подлинного источника, а само сообщение является тем же, которое было отправлено. На этом завершается аутентификация принятого сообщения. Кроме самого сообщения протокола RRC и ключа IK входами функции f9 являются:

- счетчик COUNT-I (32 бит): увеличивается на единицу после каждого нового сообщения RRC. COUNT-I состоит из старших 20 бит HFN, 8 бит со значением 0 и 4 бита последовательных номеров сообщений RRC.
- FRESH: случайное число, сгенерированное RNC. Значения COUNT-I и FRESH служат защитой от угрозы «повтор».
- бит направления (восходящее или нисходящее).

Сообщение 5 протокола RRC Security Mode Complete ("режим безопасности" установлен) указывает, что UE успешно перешло на выбранные алгоритмы защиты целостности и шифрования. После приема сообщений 5 в RNC производится аутентификация этого сообщения, т.е. проверка подлинности источника сообщений и его целостности.

В сообщения 6 RNC информирует область базовой сети о завершении установки режима безопасности. Это сообщение (Security Mode Complete) передается по протоколу RANAP. На этом завершается установление безопасной связи при передаче сигнальных сообщений между оборудованием пользователя и контроллером базовых станций.

23.3.6. Шифрование сообщений

Как было отмечено в разделе 22.3.3, TMSI/P-TMSI передаются пользователю из сети (VLR/SGSN) в зашифрованном виде. Аналогично в GSM TMSI передается на радио-участке MS в зашифрованном виде. Настоящий раздел посвящен процедуре шифрования в UMTS. На рис. 23.11 приведена схема алгоритма шифрования/дешифрования в UMTS.

Шифрованию/дешифрованию подлежат сообщения сигнализации (например, TMSI/P-TMSI, LAI) и информационные данные. Механизм шифрования основан на принципе поточного шифра. Данные открытого текста побитно суммируются по модулю 2 с псевдослучайной комбинацией. Псевдослучайная комбинация (ключевой поток) образуется с помощью одного из алгоритмов, обозначенных общей функцией f8. Выбор конкретного алгоритма производится с помощью процедуры установления режима безопасности (разд. 23.3.3.).

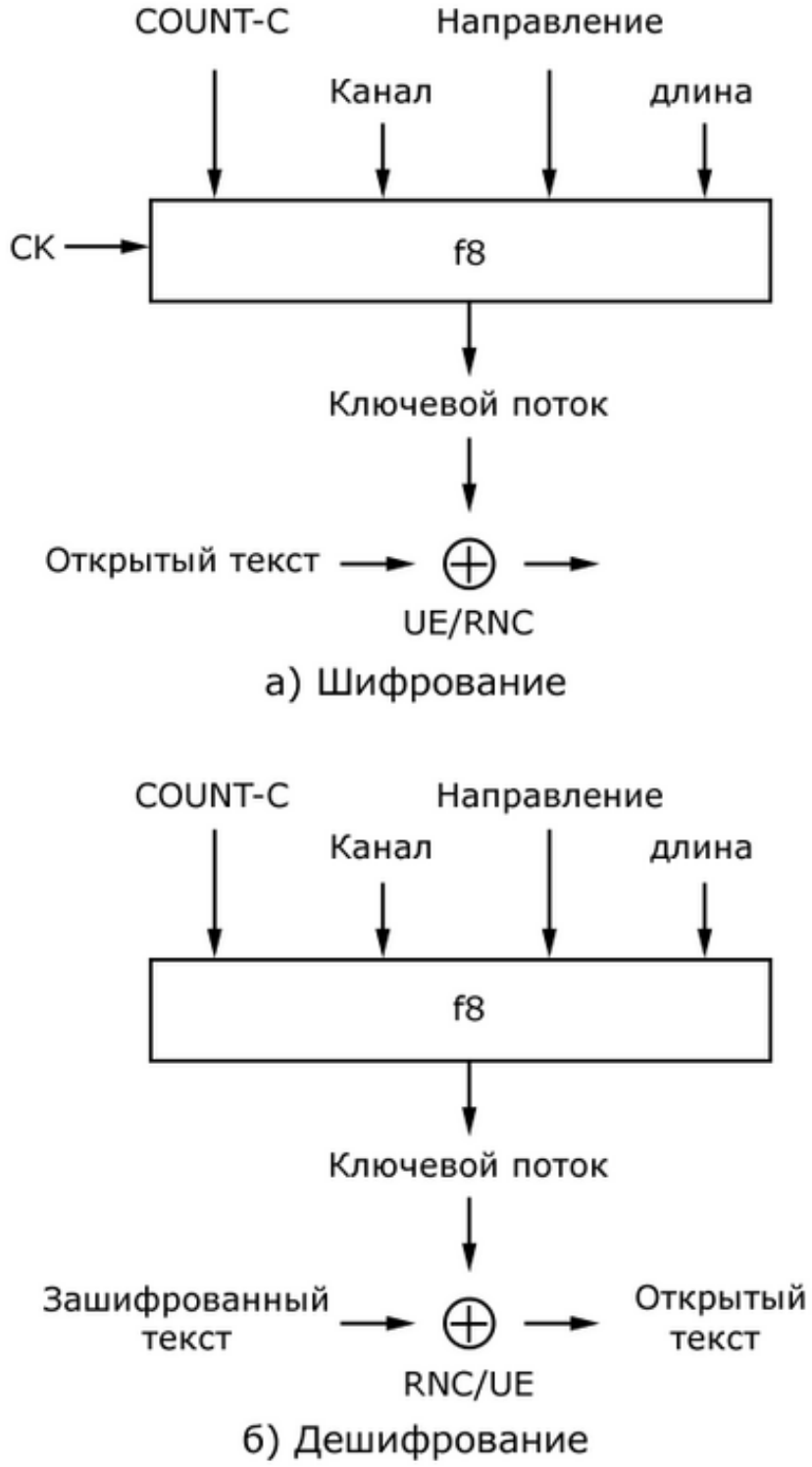


Рис. 23.11. Алгоритм шифрования/дешифрования в UMTS

Входными параметрами функции f8 являются:

- ключ шифрования СК;
- счетчик Count-C той же длины, что и счетчик Count-I для защиты целостности

данных;

- канал (идентификатор радиоканала);
- бит направления (восходящее или исходящее);
- длина. Так как данные, подлежащие шифрованию, представляют собой блоки определенной длины, то значение поля «длина» в 16 бит указывает на длину блока ключевого потока.

Счетчик Count-C выполняет функцию защиты от раскрытия зашифрованного текста. Count-C увеличивается на единицу после каждого блока ключевого потока. Таким образом, достигается шифрование двух блоков данных разными блоками ключевого потока. В противном случае (если два различных блока открытого текста шифруются одной и той же ключевой последовательностью) зашифрованные блоки легко взламываются. Для этого достаточно их сложить по модулю 2 и получить в результате сумму по модулю 2 двух блоков открытого текста. Последняя сумма легко расшифровывается. Такая же проблема может возникнуть, если не использовать идентификатор канала' при формировании ключевой последовательности.

Для защиты от угрозы «повтор» при маскировании нарушителя под UE или RNC используется процедура проверки счетчика. Для того чтобы минимизировать риск от этой угрозы, RNC может в любой момент запросить UE содержание его счетчика Count-C. Если значение Count-C UE не соответствует значению Count-C RNC, то соединение RRC сбрасывается.

Дополнения к разделу 23.3. “Информационная безопасность UMTS”

Дополнение 1. Список угроз ИБ в сети UMTS

В настоящем Дополнении приведен список, включающий большую часть угроз ИБ в сети UMTS, описание которых изложено в документе ETSI [85]. Обозначение угроз принято в соответствии с указанным документом. Все приведенные угрозы ИБ распределены в зависимости от места воздействия соответствующих им атак:

- на участке радиодоступа (радио-интерфейса);
- на других участках сети;
- в терминалах и UICC/USIM.

Под UICC (UMTS integrated Circuit Card) понимается физический прибор, который может вставляться и выниматься из оборудования терминала. Он применяется для различных приложений, одним из которых является модуль идентификации абонента USIM.

Угрозы, связанные с атаками на участке радиодоступа

Радио-участок между терминалом и обслуживающей сетью является одним из наиболее уязвимых мест воздействия атак в UMTS. Угрозы, связанные с этим участком и описанные ниже, разделены на следующие категории:

- несанкционированный доступ к данным;
- угрозы целостности данных;
- «отказ в обслуживании»;
- несанкционированный доступ к услугам.

Ниже приведены таблицы с описанием угроз ИБ. Принятые обозначения угрозы TAn соответствуют:

T – первая буква английского слова «угроза» (threat):

A – цифра соответствует номеру группы угроз (номер таблицы);

n – буква соответствует порядковому номеру угрозы в группе угроз (в соответствии со списком угроз в документе ETSI [70]).

В таблице 23.3 приведено описание некоторых угроз несанкционированного доступа к данным на радиоучастке.

Таблица 23.3.

Обозна-чение угрозы	Название угрозы	Описание угрозы
T1a	Перехват трафика пользователя	Нарушители могут перехватить трафик пользователя.
T1в	Перехват данных сигнализации и управления	Нарушители могут перехватить данные сигнализации и данные управления. Перехваченные данные могут быть использованы для доступа к данным управления безопасностью или к другой информации, которыми можно воспользоваться при проведении активных атак на систему UMTS.
T1c	Маскирование под участника	Нарушители могут маскироваться под элемент сети для того, чтобы перехватить пользовательский трафик, данные сигнализации и данные управления.
T1d	Пассивный анализ трафика	Нарушители могут наблюдать за характеристиками сообщений (время, скорость, длина, источники и назначение) для того, чтобы получить доступ к информации.
T1e	Активный анализ трафика	Нарушители могут активно инициировать соединение, а затем получать доступ к информации с помощью полученных наблюдений за характеристиками (время, скорость, длина, источники и назначение) связанных друг с другом сообщений.

В таблице 23.4 приведено описание некоторых угроз целостности информации.

Таблица 23.4.

Обозначение угрозы	Название угрозы	Описание угрозы
T2a	Манипуляция с трафиком пользователя	Нарушители могут модифицировать, вставить, повторить или уничтожить трафик пользователя. Эта манипуляция может быть случайной или намеренной.
T2в	Манипуляция с данными сигнализации или управления	Нарушитель может модифицировать, вставить, повторить или уничтожить данные сигнализации или управления.

В таблице 23.5 приведено описание некоторых угроз «отказ в обслуживании».

Таблица 23.5.

Обозначение угрозы	Название угрозы	Описание угрозы
T3a	Физическое вмешательство	Нарушители могут создать физическим способом препятствие передаче трафика пользователя, данных сигнализации и данных управления. Пример физического вмешательства может радиоглушение.
T3в	Вмешательство в протокол	Нарушители могут ввести специальные отказы в протоколе, которые создают препятствия передаче трафика пользователя, данных сигнализации и данных управления. Эти отказы в протоколе могут быть введены физическими способами.
T3c	Отказ в обслуживании в результате маскирования под участника в связи	Нарушители могут отказать в обслуживании законному пользователю, создавая препятствия трафика пользователя, данных сигнализации и данных управления. Для осуществления такого отказа нарушитель маскируется под элемент сети.

В таблице 23.6 приведено описание угрозы несанкционированного доступа к услугам.

Таблица 23.6.

Обозна-чение угрозы	Название угрозы	Описание угрозы
T4a	Маскирование под другого пользователя	Нарушитель маскируется под другого пользователя сети. Сначала нарушитель маскируется под базовую станцию в отношении пользователя. После проведения аутентификации нарушитель захватывает соединение.

Угрозы, связанные с атаками на других участках системы

Хотя атаки на радио-участке представляют наиболее серьезные угрозы, атаки на других участках системы также требуют анализа с точки зрения ИБ. Это относится к радио-участку второго пользователя, участвующего в соединении, а также к проводной части сети. При этом к категориям угроз ИБ на отдельном радио-участке добавляется категория, соответствующая отказу пользователя соединения в том, что он был его участником.

В таблице 23.7 приведено описание некоторых угроз несанкционированного доступа к данным.

Угрозы T5a, T5в, T5c, T5d не приведены в таблице, так как они аналогичны угрозам T1a, T1в, T1c, T1d таблицы 23.3. Отличие состоит лишь в том, что угрозы T5a-T5d имеют место не только на беспроводных участках системы, но и на проводных участках.

Таблица 23.7.

Обозначение угрозы	Название угрозы	Описание угрозы
T5 T5e	Несанкционированный доступ к данным на объекте системы.	Нарушители (с помощью физического воздействия или логического управления) могут получить доступ к локальным или удаленным данным.
T5f	Компрометация информации о местоположении.	Законный пользователь услуги системы UMTS может получить информацию о местоположении других пользователей системы в результате анализа данных сигнализации или голосовых сообщений, полученных при установлении соединения.

В таблице 23.8 приведено описание некоторых угроз целостности информации. Угрозы T6a и T6в аналогичны угрозам соответственно T2a и T2в. Отличие состоит в том, что угрозы T6a и T6в имеют место на только на беспроводных участках системы, но и на проводных участках.

Таблица 23.8.

Обозначение угрозы	Название угрозы	Описание угрозы
T6c	Манипуляция маскированием под участника связи.	Нарушители могут маскироваться под элемент сети для того, чтобы модифицировать, вставить, повторить или уничтожить трафик пользователя, данные сигнализации или данные управления в любом системном интерфейсе, как проводном, так и беспроводном
T6f	Манипуляция с данными на объектах системы	Нарушители могут модифицировать, вставить, уничтожить данные, которые содержатся на объектах системы. Нарушители либо физическим воздействием, либо логическим управлением могут получить доступ к данным локально или удаленно.

В таблице 23.9 приведено описание угроз ИБ, относящихся к «отказу в обслуживании».

Таблица 23.9.

Обозначение угрозы	Название угрозы	Описание угрозы
T7a	Физическое вмешательство	Нарушители могут физическими методами препятствовать передаче на любом интерфейсе системы (проводном или беспроводном участке) трафика пользователя или данных сигнализации. Например, физическим способом препятствия на проводном интерфейсе может быть обрыв провода. На проводном или беспроводном участке физическим препятствием может быть прерывание работы системы подачи питания.
T7в	Вмешательство в протокол	Нарушители могут препятствовать передаче на любом интерфейсе системы (проводном или беспроводном участке) трафика пользователя или данных сигнализации путем отказа в работе протокола. Эти протокольные отказы могут быть введены физическими методами
T7c	Отказ в обслуживании путем маскирования участников связи	Нарушители могут отказать в обслуживании пользователям путем препятствия в передаче трафика пользователя и данных сигнализации, управления путём их блокировки в результате маскирования под сетевой элемент
T7d	Неправильное использование услуг по обслуживанию аварийных ситуаций	Нарушители могут препятствовать доступу к услугам других пользователей и вызывать при этом нарушение работы оборудования по выполнению функций при аварийных ситуациях. Это может быть достигнуто нарушением услуги по обслуживанию аварийных ситуаций созданием вызовов без использования модуля USIM. Если такие вызовы удастся нарушителю позволить установить, то провайдер может не иметь способа препятствовать нарушителю доступ к обслуживанию

В таблице 23.10 приведено описание некоторых угроз, вызванных отказом одного из участников соединения в том, что он был его участником.

Таблица 23.10.

Обозна-чение угрозы	Название угрозы	Описание угрозы
T8a	Несогласие с представленным счетом	Несогласие с представленным счетом. Это может быть выражено в отказе попытки предоставления услуги или в отказе того, что услуга была действительно предоставлена.
T8в	Отказ источника трафика пользователя	Пользователь может отказаться в том, что он отправлял трафик.
T8c	Отказ доставки трафика пользователя	Пользователь может отказаться в том, что он получил трафик пользователя.

В таблице 23.11 приведено описание несанкционированного доступа к услугам.

Таблица 23.11.

Обозна-чение угрозы	Название угрозы	Описание угрозы
T9a	Маскирование под пользователя	Нарушители могут представиться пользователем для того, чтобы воспользоваться санкционированными услугами этого пользователя. Нарушитель смог получить такую возможность от других объектов таких, как обслуживающая сеть, домашняя среда и даже сам пользователь.
T9в	Маскирование под обслуживающую сеть	Нарушители могут представиться обслуживающей сетью или частью инфраструктуры обслуживающей сети для того, чтобы использовать попытки санкционированного доступа и получить самому доступ к услугам.
T9c	Маскирование под домашнюю среду	Нарушители могут представиться домашней средой для того, чтобы получить информацию, которая дает ему

		возможность маскироваться под пользователя.
T9d	Неправильное использование приоритетов пользователя	Пользователи могут неправильно использовать назначенные им приоритеты для того, чтобы получить несанкционированный доступ к услугам или просто бесплатно интенсивно использовать их подписку
T9e	Неправильное использование приоритетов обслуживающей сети	Обслуживающие сети могут неправильно использовать их приоритеты для получения несанкционированного доступа к услугам. Обслуживающая сеть могла бы, например, не использовать аутентификационные данные пользователя или замаскироваться под этого пользователя, или просто создать фальшивые счета и получить дополнительный доход от домашней среды.

Угрозы, связанные с атаками на терминал и UICC/USIM

В таблице 23.12 приведено описание некоторых угроз, связанных с атаками на терминал и UICC/USIM. В смарт-карте UICC (UMTS Integrated Circuit Card) находится модуль идентификации абонента USIM (UMTS Service Identity Module).

Таблица 23.12.

Обозна-чение угрозы	Название угрозы	Описание угрозы
T10h	Маскирование с целью приема данных на интерфейсе UICC – терминал.	Нарушители могут маскироваться под USIM или терминал для того, чтобы перехватить данные на интерфейсе UICC – терминал.
T10j	Конфиденциальность определенных данных пользователя в терминале и UICC/USIM	Нарушители могут пожелать получить доступ к персональным данным пользователя, хранимых в терминале или UICC.
	Конфиденциальность	Нарушители могут пожелать получить доступ к данным

T10k	данных аутентификации в UICC/USIM	аутентификации, хранимых провайдером услуг, например, ключ аутентификации.

Дополнение 2. Требования по защите от угроз в сети UMTS с помощью механизмов аутентификации

В настоящем приложении приведена таблица 23.13 некоторых из угроз ИБ в сети UMTS, которые требуют защиту с помощью механизмов аутентификации. Защита мобильного устройства 3G обеспечивается модулем идентификации услуг USIM (UMTS Service Identity Module).

Таблица включает номера угроз (в соответствии с Дополнением 1), описание требований по защите, и указания группы угроз по требованиям по защите.

Таблица 23.13

Номера угроз	Описание требований по защите	Группа требований по защите
T4a, T9a, T9c	Должна быть обеспечена возможность не допустить получение маскирующимся под законных пользователей несанкционированный доступ к обслуживанию 3G.	Требования по безопасности доступа к обслуживанию.
T4a, T8a, T9d, T9e	Обеспечить провайдерам услуг возможность аутентифицировать пользователей при запросе и во время предоставления услуги для того, чтобы препятствовать нарушителю получить незаконный доступ к услугам 3G в результате их маскирования или неправильного использования приоритетов.	Требования по безопасности предоставления обслуживания
T7в, T7c	Должна быть обеспечена защита от несанкционированной модификации трафика пользователя.	Требования на целостность системы
T7a, T7в, T7c	Должна быть обеспечена защита от несанкционированной модификации трафика пользователя.	Требования на целостность системы
T1a, T1b	Должна быть обеспечена пользователю возможность проверки того, что его трафик и информация о его вызовах конфиденциальны.	Требование к защите персональных данных
	Не должна быть возможность доступа к	Требование к безопасности

T10h, T10k	данным USIM, которые предназначены для использования только внутри USIM, например ключи аутентификации и алгоритмы.	USIM

Дополнение 3. Количественная оценка угроз информационной безопасности

В основу количественной оценки угрозы безопасности в UMTS положен метод, предложенный в документе ETSI ETR 332, описание которого приведено в Приложении А (раздел А3). Приведенные в документе ETSI [85] угрозы по количественной характеристике относятся к высокому, среднему или незначительному риску [86]. Угрозы T1a, T1b, T1c, T9a, T9d относятся к группе с высоким риском. Угрозы T4a, T9b относятся к группе со средним риском.

ГЛАВА 24. Беспроводные локальные сети стандартов 802.11

24.1. Архитектура сети стандарта 802.11

Стандарт IEEE 802.11 является базовым для всех последующих спецификаций (802.11a, 802.11b, 802.11g, 802.11n). Коммерческое название этих сетей — Wi-Fi (Wireless Fidelity). Эта технология используется в таких областях, как беспроводный доступ в Интернет, беспроводное телевидение. Различные стандарты семейства Wi-Fi определяют физический уровень (PHY) и подуровень управления доступом к среде (каналу) MAC (Medium Access Control). Верхние уровни совпадают по своей структуре, как для беспроводных, так и для проводных локальных сетей. Физический уровень определяет способ работы со средой передачи, скорость и методы модуляции. Подуровень MAC отвечает за распределение канала, т.е. за то, какая станция будет передавать следующей. На MAC-подуровне определён принцип, по которому устройства используют (делят) общий канал; механизм аутентификации пользователя и механизм шифрования данных. Поскольку стандарт 802.11 разрабатывался как «беспроводный Ethernet», он предусматривает пакетную передачу с 48-битовыми адресами пакетов, как и любая сеть Ethernet. Комитет IEEE 802 обеспечил совместимость всех своих стандартов. Беспроводные сети 802.11 легко сопрягаются с проводными сетями Ethernet.

Стандарт 802.11 предусматривает два основные способа (режима) организации сети [87,88]:

- с базовой станцией, называемой в терминологии 802.11 *точкой доступа AP* (Access Point). Связь между устройствами происходит только через AP. Через AP может быть выход во внешние проводные сети. Такие сети называют также структурированными или работающими в режиме инфраструктуры. Такой режим позволяет транслировать мультимедийную информацию для работы в Интернете (рис. 24.1, а). В сети 802.11 может быть несколько точек доступа, объединённых проводной сетью Ethernet (рис. 24.1, б). Фактически такая сеть представляет набор базовых станций с перекрывающимися зонами охвата. Точки доступа AP могут быть доступны к Интернету также через беспроводную сеть WiMAX (см. следующую главу).
- без базовой станции (т.е. без точки доступа), по принципу «равный с равным». Такие сети называют *беспроводными самоорганизующимися сетями Ad Hoc* (рис. 24.2). Беспроводные клиенты в этом режиме представляют независимый базовый набор служб IBSS (Independent Basis Service Set) [88]. Сети, которые поддерживают такую

архитектуру, обычно называют *беспроводными Ad Hoc сетями*. Термин Ad Hoc-по английски - for this purpuse (целевые). Мобильная Ad Hoc сеть (MANET, Mobile Ad Hoc Network) является распределённой системой из мобильных терминалов, снабженных приемо-передатчиком [89]. Они могут динамически организовывать временные сети. В сетях MANET мобильные устройства выполняют функции не только оконечных станций, но и сетевых узлов, выполняющих функции маршрутизаторов.

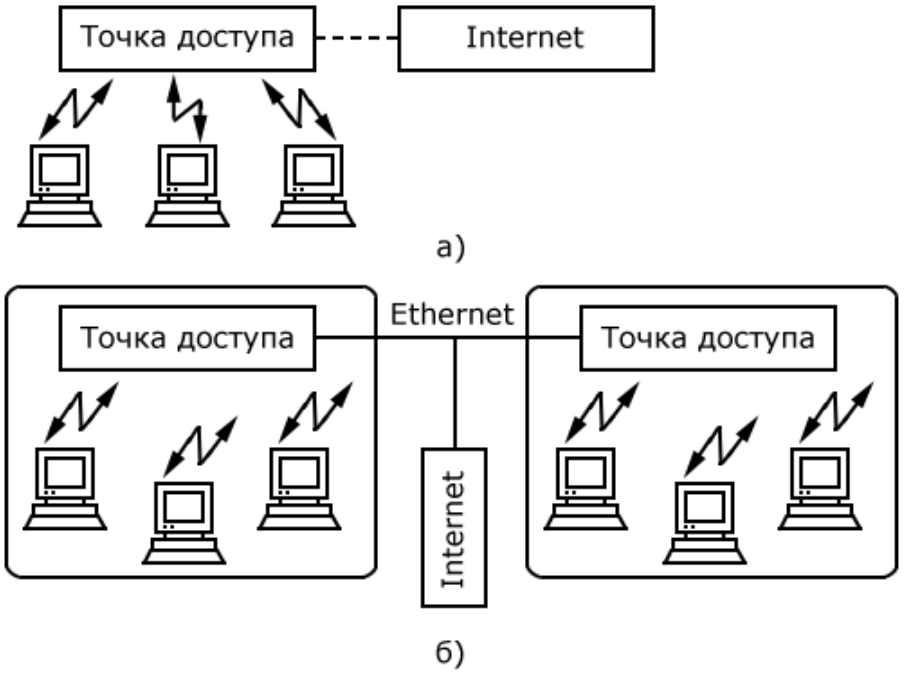


Рис. 24.1. Режим с точкой доступа

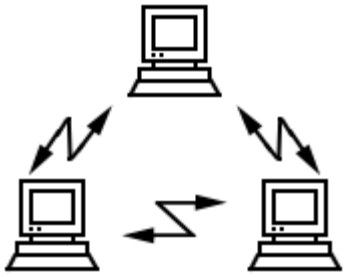


Рис. 24.2. Режим без точки доступа (сеть Ad Hoc)

Как правило, такие сети не требуют администрирования. Терминалы, которые не находятся в радиусе действия приемо-передатчиков, осуществляют передачу через

последовательность промежуточных маршрутизаторов. Сеть MANET является многошаговой (multihop) в отличие от сети с точкой доступа и может быть подключена с помощью шлюзов к фиксированной сети.

24.2. Подуровень MAC стандартов сетей Wi-Fi

Протокол подуровня управления доступом к среде (MAC) в стандарте 802.11 отличается от аналогичного протокола в проводной сети Ethernet. В Ethernet используется механизм множественного доступа к общему каналу связи с контролем несущей и обнаружением конфликтов CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Станция может начать передачу, если канал свободен. Если шумовой всплеск не приходит обратно в течение определённого времени, то кадр доставлен корректно. Таким образом, даже при передаче устройство должно контролировать канал, т.е. работать на приём. В беспроводных сетях такой способ не годится. Существуют в беспроводной сети проблемы скрытой и засвеченной станции. В результате не получается прослушать эфир и осуществить передачу только тогда, когда он никем не занят. Эти проблемы рассмотрим на участках сети, приведенных на рис. 24.3 и 24.4. Мощность передатчиков такова, что радиус действия ограничен только соседними станциями, т.е. A и B, C и B, C и D.

Рассмотрим проблему скрытой станции (рис. 24.3). Станция A передает сообщение станции B. Станция C передаёт сообщение станции B. Если станция C опрашивает канал, то она не будет слышать станцию A, находящуюся вне ее зоны действия. В результате станция C не слышит, что станция B уже занята и начнет передавать сообщение ей. В результате это сообщение исказит сообщение, принимаемое B от A.

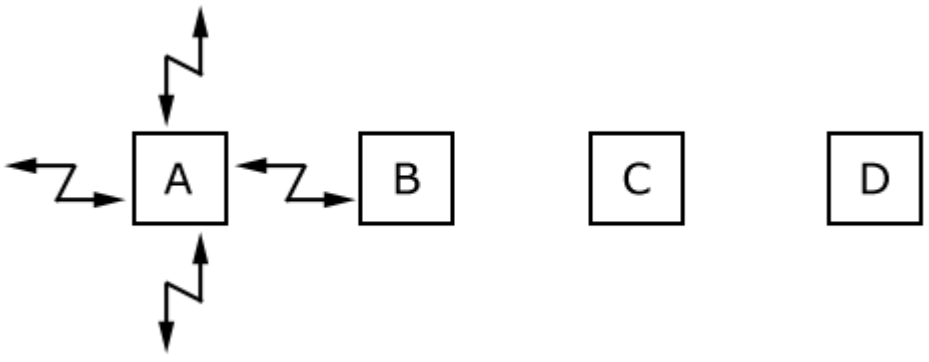


Рис. 24.3. Проблема скрытой станции

Рассмотрим проблему засвеченной станции (рис. 24.4). Станция B передает станции A сообщение. Станция C при опросе канала слышит выполняемую передачу и может ошибочно предположить, что она не в состоянии передавать данные станции D. В действительности

такая передача создала бы только помехи в зоне от станции B до станции C, где в данный момент не ведется прием.

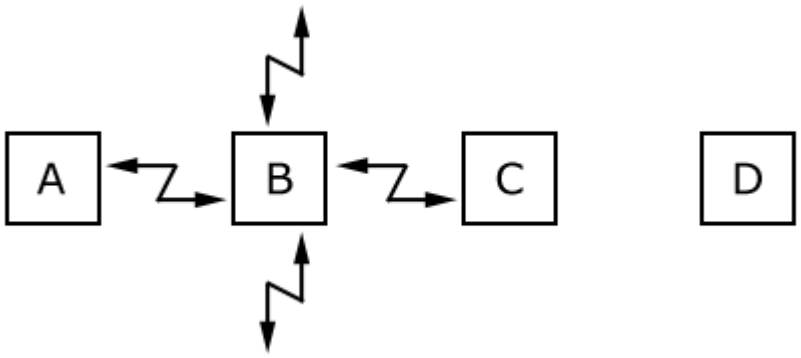


Рис. 24.4. Проблема засвеченной станции

Для устранения этих проблем в стандарте 802.11 для режима Ad Hoc без точки доступа принят режим CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) - множественный доступ с контролем несущей и предотвращением коллизий. Сети Ad Hoc должны поддерживать этот протокол. На рис. 24.5 и 24.6 показан пример использования режима CSMA/CA, основанного на протоколе MACAW. Станция D входит в зону действия B, но не входит в зону действия A. Станция C находится в зоне действия A, а также возможно в зоне действия B.

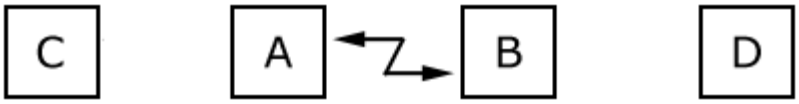


Рис. 24.5. Расположение станций примера использования протокола MACAW

На рис. 24.6. показан принцип работы протокола MACAW для предотвращения коллизий. Станция A посылает станции B кадр RTS запроса разрешения на передачу. Рассмотрим процесс с точки зрения станции A. Если B может принять данные, она отправляет в A подтверждение готовности приема – кадр CTS. После приема CTS станция A запускает таймер ACK и начинает передачу данных. В случае приема неискаженного сообщения станция B передает в A кадр о конце передачи данных ACK.

Рис. 24.6. Принцип работы протокола MACAW для предотвращения коллизий

Рассмотрим процесс с точки зрения станций C и D. Станция C находится в зоне действия A, поэтому она также принимает кадр RTS, в котором указано, сколько времени займет передача данных из A в B. В течение этого времени C считает, что канал занят, и она не должна передавать данные. Индикацией такого состояния является состояние NAV. Станция D не охвачена зоной действия A, а поэтому кадр RTS не поступает к ней. Зато кадр CTS, посланный станцией B поступает в D, которая также выставляет состояние NAV. В результате D считает канал занятым и не передает в течение определенного времени данные в адрес станции B.

Приведем основные поля кадра 802.11:

- поле управления кадром. Указывает тип кадра (информационный, контрольный, управления). Примером информационного кадра являются данные или сообщение о переходе станции в режим работы с пониженным энергопотреблением. Примером контрольного кадра являются приведенные выше кадры RTS, CTS, ACK. Кадры управления используются для управления связью станций и точек доступа (например, кадры аутентификации пользователя или отмены аутентификации);
- поле идентификатор длительности. (например, приведенное выше поле NAV);
- поле адресов. Возможны следующие типы адресов: отправителя, получателя, исходящей ячейки точки доступа, входящей ячейки точки доступа;
- поле данные. Длина данных кадра может достигать 2312 байт. Коэффициент ошибок в канале беспроводных локальных вычислительных сетях БЛВС значительно хуже, чем в проводных ЛВС. Для повышения производительности БЛВС применяется разбиение кадров на фрагменты, которые содержат собственную контрольно-проверочную сумму. Фрагментация повышает

производительность путем принудительной повторной пересылки коротких фрагментов, в которых произошла ошибка, а не кадров целиком;

- поле номер позволяет нумеровать фрагменты. Из 16 бит поля 12 идентифицируют кадр, а 4 – фрагмент;
- поле контрольно проверочная комбинация циклического кода.

24.3. Физический уровень стандартов сетей Wi-Fi

Рассмотрим физические уровни стандартов группы 802.11, которые различаются технологиями и достижимыми скоростями:

- базовый 802.11;
- 802.11b;
- 802.11a;
- 802.11g;
- 802.11n.

Важной проблемой в развитии сетей Wi-Fi является выделение соответствующей полосы рабочих частот. Быстрое развитие сетей обеспечивается при выделении диапазона частот, не требующего лицензирования. В России разрешено нелицензионное использование диапазона частот 2,4 ГГц и 5,5 Ггц. Диапазон 2,4 ГГц предусмотрен всеми стандартами рассматриваемой группы, кроме 802.11a, который допускает работу только в нелицензионном диапазоне 5 ГГц. Нелицензионный диапазон частот используется для промышленных, медицинских и научных нужд ISM (Industrial, Scientific, Medical), включая домашние радиотелефоны, СВЧ - печи и др. Поэтому высокий уровень помех потребовал отмеченную в разделе 2 фрагментацию кадров на подуровне MAC.

24.3.1. Базовый стандарт 802.11

В базовом (изначальном) стандарте 802.11 регламентируется работа оборудования на центральной частоте 2,4 ГГц с максимальной скоростью до 2 Мбит/с. На физическом уровне базового протокола 802.11 реализовано 2 метода передачи данных, позволяющие передать кадр подуровня MAC с одной станции на другую [10]:

- метод перескока частоты FHSS (Frequency Hopping Spread Spectrum);
- опционно метод расширение спектра методом прямой последовательности DSSS (Direct Sequence Spread Spectrum).

Метод FHSS аналогичен ранее рассматриваемому перескоку частоты в сети GSM и EDGE, а метод DSSS во многом напоминает ранее рассматриваемый метод в системе кодового разделения CDMA. Устройства FHSS делят предназнченную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов. Ширина каждого из 79 каналов составляет 1МГц. Отправитель и получатель согласовывают схему переключения каналов, и данные пересылаются последовательно по различным каналам с использованием выбранной схемы. Частота перескока должна быть не менее 2,5 раза в секунду между шестью каналами. Технология FHSS и DSSS обеспечивает максимальную скорость передачи данных лишь 2Мбит/с, в то время как сейчас имеются более быстродействующие сети на основе стандартов 802.11b, 802.11a, 802.11g, 802.11n.

24.3.2. Стандарт 802.11b

На физическом уровне 802.11b реализован метод высокоскоростной передачи широкополосного канала по методу прямой последовательности **HR-DSSS** (High Rate Direct Sequence Spread Spectrum). Каждый информационный бит замещается чиповой последовательностью 11 бит, равной скалярному произведению информационного бита на поледовательность Баркера длиной 11 бит B1=(10110111000). Далее сигнал кодируется посредством дифференциальной двух- или четырехпозиционной фазовой модуляции (DBPSK или DQPSK, один или два чипа на символ). При частоте модуляции несущей 11МГц общая скорость составляет в зависимости от типа модуляции 1 или 2 Мбит/с. Стандарт 802.11b предусматривает скорости передачи 11 и 5,5 Мбит/с. Для этого используется кодирование комплементарным кодом (CCK-модуляция, Complementary Code Keying), которое позволяет кодировать 8 бит на один символ, что соответствует скорости передачи 11 Мбит/с. При скорости передачи 5,5 Мбит/с в одном символе кодируется 4 бита. В протоколе также предусмотрена коррекция ошибок FEC. В расширенном варианте стандарта 802.11b+ скорость передачи данных может достигать 22 Мбит/с. В стандарте 802.11b используется мониторинг качества канала, позволяющий автоматически изменять скорость передачи данных в зависимости от уровня сигнал/помеха. Поэтому теоретическая скорость не однозначно соответствует реальной скорости передачи данных. За последние годы во всем мире резко возросло количество беспроводных устройств, использование которых иногда создавало проблему помех и перегруженности диапазона 2,4 ГГц. Сети стандарта 802.11b работают в этом нелицензионном диапазоне. Чтобы разгрузить диапазон 2,4 ГГц был разработан стандарт 802.11a для частот 5 ГГц. В этом диапазоне уровень совокупности шумов меньше. В стандарте 802.11b принят в качестве дополнительного еще один способ модуляции — пакетное бинарное сверточное кодирование PBCCC. Этот механизм позволяет

добиваться в сетях пропускную способность 5,5; 11 и 22 Мбит/с.

24.3.3. Стандарт 802.11a

В стандарте 802.11a используются две центральные частоты в районе 5 ГГц и максимальная скорость передачи составляет до 54 Мбит/с. Эта спецификация основана на принципиально ином механизме множественного доступа, чем в рассмотренных ранее в настоящих материалах стандартов беспроводных систем сотовой связи и Wi-Fi. В 802.11a в качестве основного метода расширения спектра принято мультиплексирование с ортогональным частотным разделением сигналов OFDM (Orthogonal Frequency Division Multiplexing). Технология OFDM более эффективно использует спектр и устойчива к искажениям беспроводного сигнала из-за многолучевого распространения. Данная схема делит широкую полосу спектра на множество узких, по которым передаются параллельно различные биты. В соответствии с приказом Министерства связи и массовых коммуникаций РФ №124 (2010 год) на территории РФ для стандарта 802.11a выделены две частотные полосы: 5,150-5,350 и 5,650-6,425 ГГц. В стандарте 802.11a диапазон разбивается с частотным разносом каналов 20 МГц. При этом в каждом канале имеется 52 поднесущие частоты. Из них 48 используются для передачи данных, а остальные четыре - для синхронизации. Биты кодируются для исправления ошибок. Для этого применяется сверточный код. Скорости кодирования: 1/2, 2/3, 3/4. Максимальная скорость кодирования 3/4, когда к каждым трем входным битам добавляется еще один. При использовании бинарной фазовой модуляции BPSK пропускная способность подканала 125 кбит/с. Пропускная способность всего канала с 48 информационными подканалами составляет 6 Мбит/с (48*125 кбит/с.). Квадратурная фазовая модуляция QPSK позволяет удвоить пропускную способность до 12 Мбит/с. 16-уровневая квадратурная амплитудная модуляция QAM-16, кодирующая 4 бит на один Герц несущей частоты, обеспечивает 24 Мбит/с. При использовании 64-уровневой квадратурной амплитудной модуляции QAM-64, кодирующей 8 или 10 бит на один Герц несущей частоты, обеспечивается максимальная для этого стандарта скорость - 54 Мбит/с. В таблице 24.1 приведены скорости передачи для разных комбинаций скоростей кодирования и видов модуляции сети 802.11a.

Таблица 24.1. Скорости передачи для разных комбинаций скоростей кодирования и видов модуляции сети 802.11a

Модуляция	Скорость кодирования	Скорость передачи Мбит/с
BPSK	1/2	6
BPSK	3/4	9
QPSK	1/2	12
QPSK	3/4	18
QAM-16	1/2	24
QAM-16	3/4	36
QAM-64	2/3	48
QAM-64	3/4	54

К недостаткам технологии 802.11a относятся более высокая потребляемая мощность для частот 5 ГГц, а также меньший радиус действия (оборудование для 2,4 ГГц может работать на расстоянии до 300 метров, а для 5 ГГц - около 100 м).

24.3.4. Стандарт 802.11g

Стандарт 802.11g является улучшенной версией 802.11b. Он предназначен для работы на частотах 2,4 ГГц с максимальной скоростью 54 Мбит/с. Он аналогичен стандарту 802.11a по частоте и стандарту 802.11a по максимальной скорости. В нем допускается расширение спектра DSSS и OFDM. Выделенная для 802.11g полоса частот в РФ составляет 2400-2483,5 МГц.

24.3.5. Стандарт 802.11n

Стандарт 802.11n предназначен для повышения скорости передачи данных и увеличения дальности передачи информации. Он основывается, как и стандарт 802.11a на технологии OFDM и предусматривает использование в России обоих центральных частот (2,4 и 5 ГГц). При этом в РФ выделены следующие полосы частот:

- 2400-2483,5 МГц;
- 5150-5350 МГц;
- 5650-6425 МГц.

Повышение скорости передачи информации в этом стандарте достигается за счет следующих мер.

- Удвоение полосы пропускания канала с 20 до 40 МГц, при этом режим 20 МГц — обязательный и для него установлен базовый режим скоростей передачи. В таблице 24.2 приведены скорости передачи для разных комбинаций скоростей кодирования и видов модуляции сети 802.11n при полосе 20 МГц [90,91]. При полосе канала 40 МГц пропускная способность канала почти удваивается, поскольку при прочих равных условиях почти удваивается и число поднесущих (вместо 52 их становится 108). Уменьшение защитного интервала с 800 нс до 400 нс также увеличивает скорость передачи информации.

- Применение технологии многоканальных антенных систем MIMO (Multiple Input Multiple Output), т.е. множественные входы и множественные выходы. В основу положено применение нескольких передающих и приемных антенн. Передаваемый поток данных разбивается на независимые последовательности битов, которые пересылаются одновременно с использованием разных антенн. С помощью нескольких антенн система MIMO позволяет осуществлять пространственное мультиплексирование потоков, что обеспечивает повышение скорости передачи данных. Система MIMO позволяет также по нескольким антеннам (до четырех) передавать одновременно один и тот же поток данных. По причине многолучевого распространения приёмник получает несколько сигналов. С помощью технологии MIMO эти сигналы обрабатываются и из них восстанавливается исходный сигнал, что способствует улучшению соотношения сигнал/помеха. Так оборудование стандарта 802.11n с несколькими передающими и принимающими антеннами позволяет повысить скорость передачи данных, улучшая при этом соотношение сигнал/помеха.

Таблица 24.2. Скорости передачи для разных комбинаций скоростей кодирования и видов модуляции сети 802.11n при полосе 20 МГц

Модуляция	Скорость кодирования	Скорость передачи Мбит/с
BPSK	1/2	7,2
QPSK	1/2	14,4
QPSK	3/4	21,7
QAM-16	1/2	28,9
QAM-16	3/4	43,3
QAM-64	2/3	57,8
QAM-64	3/4	65,0
QAM-64	5/6	72,2

24.4. Mesh-сети стандарта 802.11s

Стандарт 802.11s предназначен для беспроводных mesh – сетей WMN (Wireless mesh network). Их называют ячеистыми сетями. Беспроводные mesh-сети называют также MBSS (Mesh BSS, Mesh Basis Service Set). Mesh-сети - новый перспективный класс широкополосных беспроводных сетей передачи мультимедийной информации, который находит широкое применение при построении локальных и распределенных городских беспроводных сетей. Для WMN характерен принцип самоорганизации построения архитектуры, самоконфигурации, самовосстановления, высокой масштабируемости и надежности [92]. WMN отличает от MANET в том, что включает дополнительно отдельную опорную сеть (backbone) из маршрутизаторов, которая и предоставляет ей преимущества перед MANET. На рис. 24.7 приведена архитектура mesh-сети стандарта 802.11s, включающая маршрутизаторы (mesh-routers) [93]. Сеть backbone обычно является фиксированной. Она так же, как и MANET является многошаговой (multihops) и может быть использована для быстрого развертывания в чрезвычайных экстренных ситуациях. По сравнению с мобильными сетями Ad Hoc mesh-сети имеют преимущества в отношении надежности, пропускной способности, подверженности зашумлению. WMN обеспечивает такие возможности, как устойчивость сети при отказе отдельных компонентов, масштабируемость сети, увеличение зоны информационного покрытия в режиме самоорганизации, динамическую маршрутизацию трафика; ретрансляцию кадров между устройствами, не

имеющими между собой прямой видимости [89]. Достоинства mesh - сети: минимальное время и простота развёртывания благодаря самоорганизации, самоадаптации и самовосстановления в обход повреждённого участка, способность обеспечить связь на территории, где традиционные системы не могут это выполнить.

Отметим, что изменения в стандарте IEEE 802.11s не затрагивают физический уровень. Все нововведения относятся к MAC-уровню. Кроме того, в стандарте IEEE 802.11s рассматриваются вопросы маршрутизации пакетов в рамках mesh-сети (фактически - сетевой и транспортный уровень модели OSI).

Структура пакетов MAC-уровня в mesh-сети отличается от стандартного формата пакетов сетей 802.11 наличием mesh-заголовка. Для каждого установления соединения предусмотрено отдельное поле в заголовке - время жизни пакета при многошаговой пересылки. Это помогает бороться с зацикливанием. Для борьбы с дубликатами при пересылке предусмотрено поле нумерации пакетов.

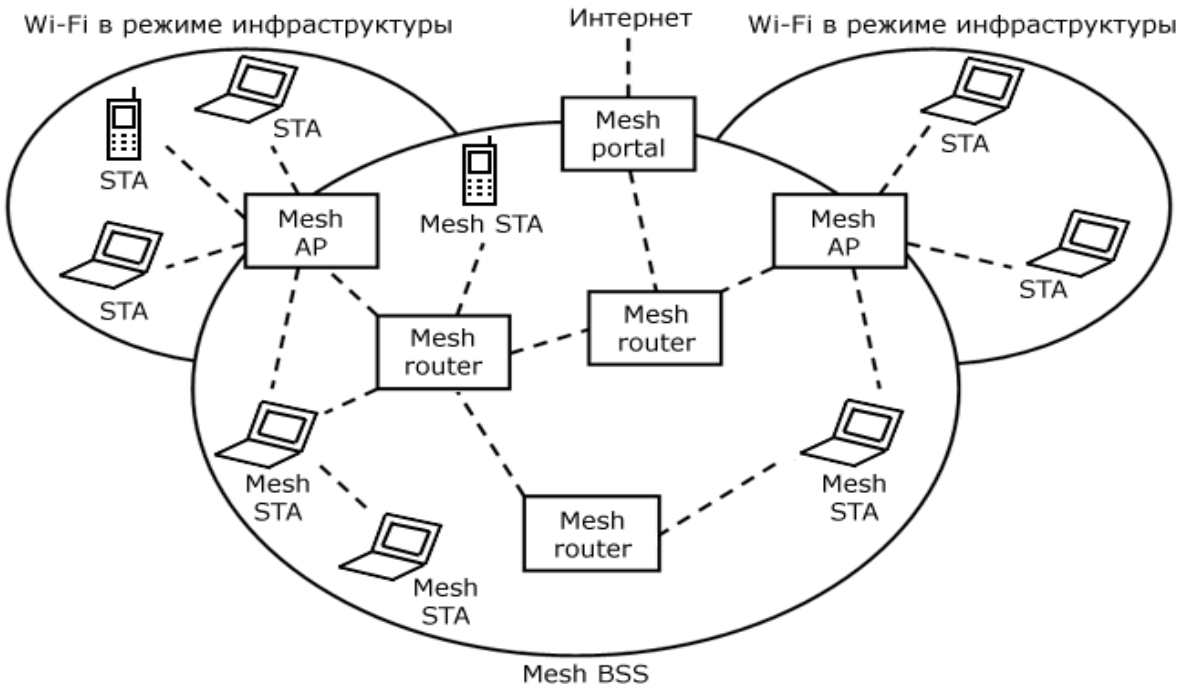


Рис. 24.7. Архитектура mesh-сети 802.11s

Приведенные на рис. 24.7 устройства выполняют следующие функции.

Mesh-router. Маршрутизатор сети маршрутизаторов, выполняющий функцию маршрутизации. Имеют несколько интерфейсов и дополнительные источники питания.

Mesh STA. Терминальные mesh-станции, выполняющие трансляцию и маршрутизацию в соседние узлы.

STA. Терминальные станции сети стандартов группы 802.11 в режиме инфраструктуры.

Mesh AP. Выполняет функцию точки доступа инфраструктурного режима для подключенных клиентов и функцию маршрутизации с узлами сети маршрутизаторов.

Mesh portal (MP). Выполняет функцию Mesh STA по обеспечению моста к различным сетям. Например, MP может быть шлюзом к WiMAX или UMTS для доступа к Интернету. Для MP характерны большие потоки трафика от пользователей mesh-сетью. Механизм установки соединений IEEE 802.11s основан на периодической посылке стандартного сообщения «открыть соединение». В ответ на него может быть получено сообщение «подтверждение соединения» или «закрытие соединения». Соединение между двумя соседними MP считается установленным тогда и только тогда, когда оба MP послали друг другу команды «открыть соединение» и ответили подтверждением соединения (в любой последовательности). Для каждого установления соединения предусмотрено время жизни, в течение которого оно должно быть использовано. Сеть стандарта определена для малых ячеистых размеров с максимальным числом узлов 64 [93].

24.5. Стандарты информационной безопасности сети Wi-Fi

В процессе совершенствования технологии информационной безопасности сети Wi-Fi последовательно были разработаны стандарты WEP, WPA и 802.11i для режима с точкой доступа.

23.5.1. Протокол безопасности WEP

Протокол *WEP* (Wired Equivalent Privacy - секретность эквивалентная проводным сетям) является частью стандартов группы 802.11 и предназначен для обеспечения информационной безопасности сетей Wi-Fi.

На рис. 24.8 представлен процесс шифрования/дешифрования и контроль целостности сообщений по этому протоколу. Контрольно-проверочная комбинация (КПК) - это 32-битовая последовательность циклического кода, присоединённая к концу кадра с целью обнаружения искажений данных в канале. Для процесса шифрования 40-битовый секретный ключ делится между двумя общающимися сторонами. К секретному ключу присоединяется вектор

инициализации (IV) длиной 24 бит, на основании которых по протоколу RC4 образуется начальное число для генератора псевдослучайной последовательности (ПСП). На рис. 24.8 это ключевая последовательность обозначена через Z.

Побитовое сложение по модулю 2 этой ключевой последовательности Z и открытого текста P с КПК создаёт зашифрованное поточным шифром сообщение $Z \oplus (P||КПК)$, которое передаётся в канал (рис. 24.8, а). Вектор инициализации передается по каналу незашифрованным. Вектор инициализации периодически меняется (при каждой новой передаче), следовательно, меняется и псевдослучайная последовательность, что усложняет задачу расшифровки перехваченного текста.

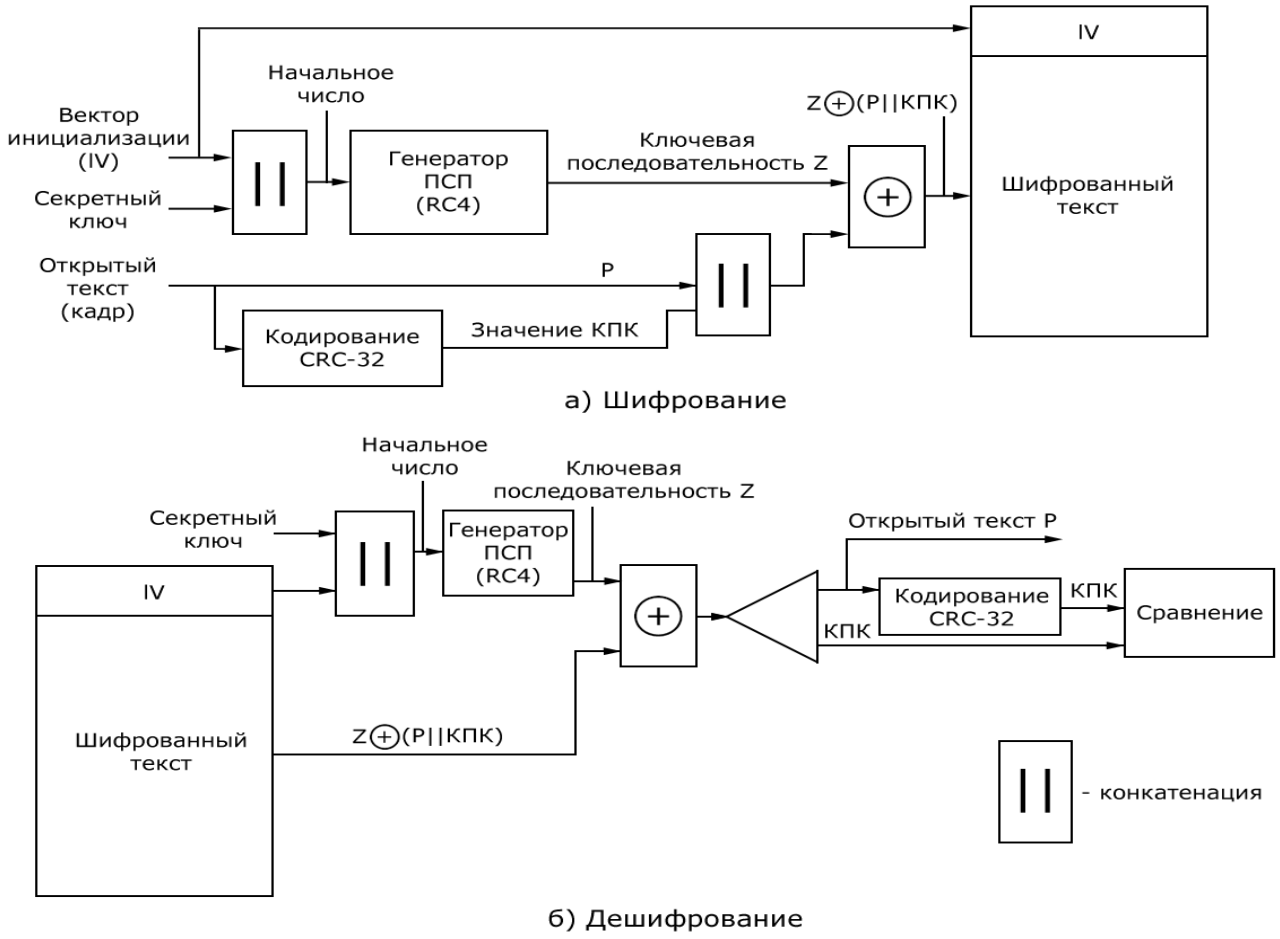


Рис. 24.8. Шифрование/дешифрование и контроль целостности сообщений по протоколу WEP

После получения сообщения (рис. 24.8, б) приёмник извлекает вектор инициализации, присоединяет его к совместно используемому секретному ключу, после чего генерирует ту

же псевдослучайную последовательность, что и источник. К полученному таким образом ключу и поступившим данным побитно применяется операция сложения по модулю 2, результатом которой является исходный текст:P||КПК $\oplus$ Z $\oplus$ Z=P||КПК. Таким образом, если взять исходный текст, применить к нему и ключевой последовательности операцию исключающего «ИЛИ», а затем применить операцию исключающего «ИЛИ» к результату и той же ключевой последовательности, то в итоге получится исходный текст. В заключение приёмник сравнивает поступившую последовательность КПК и КПК, вычисленную по восстановленным данным. Если величины совпадают, данные считаются неповреждёнными. Основным недостатком WEP является отсутствие методов создания и распространения ключей шифрования. Эти ключи должны распространяться по какому-либо секретному каналу, не использующему протокол 802.11. На самом деле, ключи шифрования WEP представляют собой обычные текстовые строки, вводимые с клавиатуры и используемые равно для беспроводных точек доступа и беспроводных клиентов. Недостатком протокола управления ключами WEP является принципиальное ограничение в предоставлении безопасности 802.11, особенно в режиме инфраструктуры с большим количеством станций. Примерами таких сетей являются корпоративные сети или сети аэропортов и других подобных заведений. Все точки доступа и беспроводные клиенты используют один и тот же вручную сконфигурированный ключ для всех сессий. При наличии множества беспроводных клиентов, передающих большое количество данных, атакующий может удалённо перехватить эти зашифрованные данные и использовать криптоаналитические методы для определения ключа шифрования WEP.

Но даже, если всем пользователям раздать разные ключи, WEP всё равно может быть взломан. Так как ключи не изменяются в течение больших периодов времени, стандарт WEP рекомендует изменять вектор инициализации при передаче каждого пакета во избежание атак посредством повторного использования. Однако ограниченная длина вектора инициализации (24 бита) позволяет злоумышленнику раскрыть зашифрованные сообщения. Прослушивая канал, злоумышленник сможет захватить два сообщения с одинаковыми векторами инициализации и ключами. Складывая их по модулю 2, он получит сумму открытых текстов, которая может быть использована для восстановления исходных данных каждого сообщения. Существуют способы для реализации такой атаки злоумышленника. Протокол WEP также выполняет функцию аутентификации оконечной станции, однако её нельзя считать не лишённой больших недостатков. К ним, в частности, относятся следующие:

- Так как общий ключ вводится на беспроводном участке для каждого беспроводного клиента вручную, этот метод не подходит для больших и сложных (корпоративных)

сетей.

- Другой серьезной проблемой данного метода является то, что для простоты один и тот же ключ используется как для аутентификации, так и для шифрования всех данных, которыми обмениваются аутентифицирующийся клиент и аутентифицирующий компьютер. Аутентификация включает передачу текста от клиента в открытом (незашифрованном) и клиенту в зашифрованном виде по протоколу WEP. Атакующий может перехватить оба варианта текста и с помощью криптоанализа вычислить общий ключ, который является также и шифрующим ключом WEP. Ну а после определения шифрующего ключа WEP атакующий получит полный доступ к беспроводной сети и сможет атаковать станции.
- Обычно ключ WEP применяется всеми пользователями беспроводной сети, что не позволяет аутентификацию отдельных пользователей.
- Аутентификации подлежат только оконечные станции. Это позволяет злоумышленнику использовать атаки с фальшивыми точками доступа.

Учитывая недостатки протокола WEP , был разработан новый протокол информационной безопасности для сетей группы стандартов IEEE 802.11 – протокол WPA.

24.5.2. Протокол безопасности WPA

Стандарт WPA (Wi-Fi Protected Access) представляет собой подмножество спецификаций из принятого в 2004 году стандарта IEEE 802.11i. Весь же набор спецификаций стандарта IEEE 802.11i Wi-Fi Alliance называется WPA2. Спецификации WPA были призваны дать пользователям альтернативу для WEP и стали переходной ступенью между ним и новым стандартом IEEE 802.11i. Структуру WPA можно представить в виде формулы WPA = IEEE 802.1X + EAP + TKIP + MIC, т. е. WPA является суммой нескольких элементов, рассмотренных ниже.

24.5.2.1. Аутентификация

Протоколы IEEE 802.1X и EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации) обеспечивают механизм аутентификации пользователей, которые должны предъявить мандат или свидетельство для доступа в сеть. В больших корпоративных сетях для аутентификации часто используют сервер **RADIUS**. Название сервера и одноименного протокола RADIUS складывается из первых букв слов — Remote Authentication Dial in User Service (услуга удаленной аутентификации вызывающего пользователя). В иерархии сети он находится выше точки доступа и содержит базу данных со списком пользователей, которым разрешен доступ к сети. В базе данных содержится необходимая для аутентификации законных пользователей информация.

Для аутентифицированного доступа в сеть Ethernet стандарт 802.1X определяет управление доступом, основанное на сетевых портах. Стандарт 802.1X включает следующие понятия: аутентификатор (точка доступа), аутентифицирующийся (беспроводный клиент), сервер аутентификации (его функцию обычно выполняет RADIUS- сервер). В стандартах 802.1X аутентификация пользователей выполняется по протоколу EAP (Extensible Authentication Protocol). Протокол 802.1X позволяет клиенту вести диалог с сервером аутентификации и видеть результат, а протокол EAP описывает, как взаимодействует клиент и сервер аутентификации. Существует несколько протоколов EAP [94]. Одним из них является EAP-TLS (RFC 2716), основанный на протоколе транспортного уровня TLS (см. глава 13). EAP-TLS обеспечивает взаимную аутентификацию беспроводного клиента и сервера аутентификации, а также создает общие ключи беспроводного пользователя и точки доступа. Протокол EAP-TLS основан на сертификатах. Ниже приводится процесс аутентификации беспроводного пользователя Wi-Fi в режиме с точкой доступа [88]. На рис. 24.9 приведены компоненты аутентификации пользователя. Аутентификация основана на сертификатах (см. главы 13,17).

- Точка доступа AP посылает запрос беспроводному пользователю запрос на установление соединения EAP-Request/Identity. Если же беспроводный пользователь начинает установление соединение с беспроводной точкой доступа, то, наоборот, он посылает сообщение EAP-Start. Беспроводная точка доступа в ответ передает сообщение EAP-Request/Identity.
- Пользователь посылает в ответ сообщение EAP-Responce/Identity, содержащее имя компьютера. Точка доступа переправляет это сообщение RADIUS-серверу в виде сообщения RADIUS Account-Request.

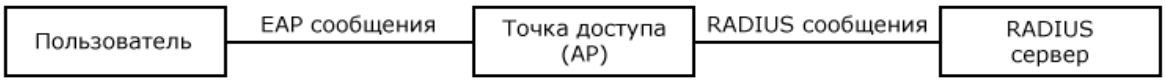


Рис. 24.9. Компоненты аутентификации пользователя

- Сервер RADIUS посылает сообщение RADIUS Access-Challenger, содержащее сообщение EAP-Request и указывающее тип EAP, что означает начало аутентификации. В данном примере этот тип EAP-TLS. Точка доступа переправляет сообщение беспроводному пользователю (в виде сообщения EAP-Request).
- Беспроводный пользователь подтверждает начало аутентификации по протоколу TLS, посылая сообщение EAP-Response с типом EAP-TLS. Точка доступа переправляет это сообщение EAP RADIUS-серверу (в виде сообщения RADIUS Access-Request).
- Сервер RADIUS посылает сообщение RADIUS Access-Challenger, содержащее сертификат (цепочку сертификатов, см. Приложение Г) сервера RADIUS. Точка доступа переправляет это сообщение беспроводному пользователю (в виде сообщения EAP-Request).
- Беспроводный пользователь посылает сообщение EAP-Response с типом EAP-TLS, содержащее свой сертификат (цепочку сертификатов). Точка доступа переправляет это сообщение серверу RADIUS.
- Сервер RADIUS посылает сообщение о завершении обмена аутентифицирующими сообщениями по протоколу TLS. Точка доступа переправляет это сообщение беспроводному пользователю.
- Беспроводный пользователь посылает сообщение подтверждения приема, которое транслируется в RADIUS-сервер.
- RADIUS-сервер, исходя из данных на предыдущих этапах, вычисляет сессионный ключ для данного пользователя и ключ для обеспечения целостности сообщений. Затем он посылает беспроводной точке доступа сообщение об аутентификации пользователя (RADIUS Access-Accept), содержащее сообщение EAP-Success и зашифрованные эти ключи. В сообщении EAP-Success об успешном приеме ключей отсутствуют ключ для шифрования данных и ключ для обеспечения целостности данных. После получения от точки доступа сообщения EAP-Success пользователь, исходя из данных на предыдущих этапах, вычисляет сессионный ключ для данного

пользователя и ключ для обеспечения целостности сообщений. Следовательно, и пользователь, и беспроводная точка доступа имеют одинаковые ключи для шифрования и обеспечения целостности данных.

- Беспроводная точка доступа посылает пользователю сообщение EAPOL (EAP over LAN)-KEY, содержащее широковещательный/глобальный ключ, зашифрованный сессионным ключом пользователя по протоколу RC4. Отдельные части сообщения EAPOL подписываются с помощью протокола (не использующего шифрование [10]) HMAC посредством ключа пользователя, обеспечивающего целостность. После приема сообщения EAPOL-KEY пользователь проверяет его целостность и расшифровывает широковещательный/глобальный ключ.

Приведенный сценарий аутентификации с сервером аутентификации для домашней сети и маленьких фирм не используется. Здесь отсутствует сервер аутентификации. Вместо него есть общий пароль, который используется для доступа в сеть. При этом для каждого клиента создается свой ключ, но у них одинаковый пароль, что позволяет узнать ключи друг друга. При использовании сервера аутентификации каждый клиент получает при успешной аутентификации, который неизвестен другим клиентам. Этот ключ используется для шифрования данных.

24.5.2.2. Конфиденциальность и целостность данных

Протокол TKIP (Temporal Key Integrity Protocol — протокол временной целостности ключа) выполняет функции обеспечения конфиденциальности и целостности данных. Функционально TKIP является расширением WEP (рис. 24.10). Аналогично WEP, он использует алгоритм шифрования RC4, но более эффективный механизм управления ключами. Протокол TKIP генерирует новый секретный ключ для каждого передаваемого пакета данных. Изменен и сам механизм генерации ключа. Он получается из трех компонентов: базового ключа длиной в 128 бит (TK), номера передаваемого пакета (TSC) и MAC-адреса устройства-передатчика (TA). Также в TKIP используется 48-разрядный вектор инициализации, чтобы избежать повторного использования IV, на котором основана выше описанная атака.

Рис. 24.10. Шифрование по протоколу TKIP

Алгоритм TKIP использует сквозной счетчик пакетов (TSC) длиной 48 бит. Он постоянно увеличивается, сбрасываясь в 1 только при генерации нового ключа. Базовый ключ для шифрования, а также для аутентификации создаётся с помощью асимметричной криптографии с использованием протокола TLS (глава 13). EAP-TLS основан на сертификатах и является надежным методом, обеспечивающим взаимную аутентификацию, определение шифрующих ключей, целостность сообщений.

Как следует из названия механизм MIC (Message Integrity Check) обеспечивает в WPA проверку целостности сообщений. MIC с помощью алгоритма Michael позволяет вычислить хеш-функцию длиной 64 бит, используя для этого, кроме данных сообщения MAC адреса источника и пункта назначения. Этот механизм более защищён от атак злоумышленника по подделке сообщения, чем используемое циклическое кодирование в протоколе WEP .

24.5.3. Протокол безопасности 802.11i

Принятый в 2004 году, стандарт 802.11i во многом сходен с WPA , однако обеспечивает более высокий уровень ИБ. Протокол 802.11i использует в качестве основного более надежный протокол CCMP (Counter – Mode CBC MAC Protocol) на базе блочного шифра стандарта AES (Advanced Encryption Standart) [10]. Протокол CCMP выполняет правила, по которым производит шифрование блочный протокол AES (подобно тому, что протокол TKIP использует протокол шифрования RC4 в WPA) [91]. Сообщения зашифровываются в режиме

счетчика (приложение Б). Для обеспечения целостности сообщений используется код аутентичности сообщения MAC (приложение Г). При этом используется другой режим шифрования (режим шифрования обратной связи, который в Приложении Б не приводится). Последний зашифрованный блок длиной 128 бит является кодом аутентичности MAC.

Для работы по стандарту 802.11i создается иерархия ключей, включающая мастер ключ МК, главный попарный ключ РМК, попарный переходный ключ РТК, главный групповой ключ GMK, групповые ключи GTK. После аутентификации беспроводного клиента сервер аутентификации и беспроводный клиент создают общий мастер ключ МК. Попарный ключ РМК создается для каждого пользователя и точки доступа RADIUS-сервером.

Ключ сеанса рассчитывается следующим образом. Точка доступа посылает в сообщении 1 случайное число nonce (“number used once”, номер, использующийся только один раз). Клиент в сообщении 2 отправляет в адрес точки доступа зашифрованный мастер ключом этот nonce. Если после расшифровки nonce совпадает с отправленным, точка доступа допускает клиента в сеть. В сообщении 3 точка доступа отправляет в адрес клиента зашифрованный мастер ключом сессионный ключ Ks. Этот ключ создается из MAC-адреса и нонса. Клиент в ответном сообщении 4 подтверждает получение сеансового ключа. Сессионный ключ действительный на определенное время, по истечении которого точка доступа отправляет новый сессионный ключ клиенту. Случайное число nonce может быть отправлено незашифрованным, так как по ним невозможно рассчитать сессионный ключ без знания мастер ключа. Для того чтобы удостоверится клиентам и точке доступа в верности сессионных ключей точка доступа передает всем подключенным к ней клиентам зашифрованное широковещательное сообщение группового ключа.

ГЛАВА 25. Сети WiMAX и LTE

25.1. Общие положения

Сети беспроводного доступа, реализующие стандарты семейства IEEE 802.16 получили название WiMAX (World Interoperability for Microwave Access, всемирная совместимость при высокочастотном доступе). На сегодня основными являются две версии стандарта: 802.16-2004 (фиксированный доступ) и 802.16e - 2005 (мобильный доступ). Стандарт 802.16e-2005 вобрал в себя всё лучшее стандарта 802.16-2004 и считается ориентированным на предоставление услуг широкополосной передачи данных мобильным пользователям. Сети WiMAX имеют сотовую структуру. Стандарт WiMAX позволяет создать технологию уровня связи (для объединения многих подсетей Wi-Fi и предоставления им доступа в Интернет), а также технологию «последней мили» (конечного отрезка от точки входа в сеть провайдера до компьютера пользователя) [87]. Действующая в настоящее время первая редакция стандарта 802.16e предусматривает следующие режимы обслуживания.

- Fixed WiMAX – фиксированный доступ. Данный режим обеспечивает гарантированную связь для неподвижного пользователя;
- Nomadic WiMAX – сеансовый доступ. Здесь подразумевается, что пользователь может передвигаться в определённой области, обслуживаемой одной базовой станцией. Если же он выходит за пределы базовой станции, то связь прерывается и устанавливается заново в новой зоне. Иногда такой доступ называют *беспроводным*;
- Portable WiMAX – в режиме перемещения. Связь гарантирована в любом месте использования. Сеанс не прерывается при перемещении между сотами через много базовых станций со скоростью до 120 км/час.
- Mobile WiMAX – мобильный доступ в режиме перемещения. Скорость передвижения не ограничена (например, в поезде со скоростью 350 км/час). Сеанс связи не прерывается при перемещении между сотами.

Радиус действия базовой станции в соте составляет для фиксированного доступа 5-8 км, максимум 50 км. Для мобильных станций радиус 1-5 км. WiMAX беспроводного фиксированного доступа с широкой полосой пропускания является конкурентом провайдерам фиксированной высокоскоростной связи в городе или сельской местности.

Приведём основное применение WiMAX:

- доступ абонентских терминалов фиксированной и подвижной служб сети Wi-Fi в сети Интернет, ТфОП, сети передачи данных. WiMAX является транзитной сетью для этих терминалов;
- доступ в сети Интернет, ТфОП, сети передачи данных абонентских терминалов напрямую через WiMAX.

В WiMAX предусмотрена также как и в Wi-Fi стандартов 802.11a,n (глава 24) технология многоканальных антенных систем MIMO, способствующая увеличению пропускной способности и/или качества обслуживания за счет увеличения соотношения сигнал/помеха.

Стандарт 802.16 определяет две топологии WiMAX:

- **«точка-многоточие»**, когда базовая станция (БС) общается со многими абонентскими станциями (АС). Трафик в этом случае существует только между БС и АС;
- **mesh-сеть**. В WiMAX предусмотрена также как и в Wi-Fi (глава 24) технология взаимодействия между собой абонентских станций АС. В этом случае АС называется узлом (node) сети. Основная разница между подуровнями MAC в WiMAX и Wi-Fi состоит в том, что WiMAX mesh-сети основаны на множественном доступе с временным делением TDMA, которые представляют распределенное по расписанию деление временных слотов. Это позволяет избежать коллизий при обращении терминалов к mesh-сети [91]. Для устранения этих проблем в Wi-Fi в режиме с точкой доступа принят механизм CSMA/CA (глава 24).

Преимуществом WiMAX mesh-сети является то, что базовая станция может быть соединена с более удалённой абонентской станцией АС.

25.2. Физический уровень WiMAX

Передача данных на физическом уровне осуществляется посредством передачи непрерывной последовательности кадров фиксированной длины. Каждый кадр состоит из двух субкадров: субкадр нисходящего (от БС к АС) и восходящего (от АС к БС) каналов. Стандартом предусмотрено как частотное *FDD (Frequency Division Duplex)*, так и временное *TDD (Time Division Duplex)* разделение трафиков восходящего и нисходящего каналов (соответственно частотный и временной дуплекс).

При временном дуплексировании каналов кадры передаются в одном частотном диапазоне, сначала нисходящий, затем восходящий. При частотном дуплексировании восходящий и нисходящий субкадры транслируются одновременно, но с частотным разносом. Рассмотрим используемые в WiMAX режим модуляции OFDM, режимы множественного доступа.

25.2.1. Режим OFDM

Напомним, что OFDM – ортогональное частотное разделение каналов. Это метод высокоскоростной передачи, при котором последовательный поток информации из N символов разбивается на n блоков по N/n символов в каждом, причём символы разных блоков передаются «параллельно», каждый на своей поднесущей. Преимущество данного метода состоит в том, что он позволяет снизить межсимвольные искажения, возникающие в канале. Кроме данных, в OFDM-символе передаётся защитный интервал длительностью $T_в$, так что общая длительность OFDM-символа $T_S = T_в + T_д$, где $T_д$ – длительность передачи данных в одном OFDM-символе. Защитный интервал представляет собой копию оконечного фрагмента символа. Его длительность Тд для OFDM согласно 802.16-04 может составлять 1/8, 1/16 и 1/32 длительности T_S. Модуляция OFDM основана на двух принципах: разбиение одного канала на N «параллельных» и измерение характеристик канала. На каждой поднесущей производится канальное кодирование, включающее скремблирование, помехоустойчивое кодирование, перемежение и модуляцию.

Из 200 поднесущих - 8 поднесущих являются пилотными для измерения характеристик канала для автоматического переключения на другую скорость канала. Остальные 192 поднесущие для передачи данных распределены на 16 логических подканалов по 12 поднесущих в каждом. Это в стандарте получило название субканального режима и изложено в качестве опционального использования, которое можно рассматривать как упрощенное приближение к мультиплексированию - множественному доступу OFDMA, который подлежит рассмотрению ниже.

25.2.2. Режим OFDMA и SOFDMA

Режим множественного доступа OFDMA (Orthogonal Frequency Division Multiple Access) аналогичен OFDM с точки зрения формирования модуляционных символов. Различие проявляется в принципе разделения каналов. Один логический канал OFDMA-канал образован фиксированным набором поднесущих в диапазоне частот физического канала. В OFDMA различные поднесущие назначаются разным пользователям. Для этого поднесущие

OFDMA разделены на подмножества. Каждое такое подмножество поднесущих является субканалом. Используется тот же метод, что и рассмотренный выше опционально используемый субканальный режим в OFDM на 16 подканалов. Ширина физического канала не нормируется (в стандарте говорится не менее 1 МГц). В OFDMA число поднесущих значительно больше, чем в OFDM – 2048. В результате число число подканалов становится достаточным для организации работы сети: в разных режимах их от 32 до 70, по 24 или 48 информационных несущих в каждом. Метод формирования символов, включающий скремблировании, кодирование, перемежение и модуляцию приведен в следующем подразделе. Режим OFDMA, обеспечивающий масштабируемость, получил название масштабируемого OFDMA (SOFDMA). SOFDMA позволяет выбрать число поднесущих из следующего набора: 2048, 1024, 512 и 128. Для мобильного WiMAX обязательными являются 1024 и 512 поднесущих, причём ширина полосы пропускания канала соответственно 10 МГц и 5 МГц. Режим с 256 поднесущими отсутствует, так как OFDMA становится аналогичным субканальному режиму в OFDM.

25.2.3. Канальное кодирование

На рис. 25.1 приведена схема стадий канального кодирования на физическом уровне в OFDM и OFDMA.

Рис. 25.1. Схема стадий канального кодирования в OFDM и OFDMA

Канальное кодирование на физическом уровне кодирование данных включает скремблирование, помехоустойчивое кодирование, перемежение и модуляцию.

Входной поток данных скремблируется, то есть умножается на псевдослучайную последовательность. Скремблер (блок 1) исключает длинные серии символов 1 и 0, что улучшает работу синхронизации. Кроме того, скремблер выполняет функцию шифрующего устройства. Схемы скремблирования в OFDM и OFDMA практически идентичны. Блок 2 осуществляет помехоустойчивое кодирование потока данных. Применяются несколько типов кодов, среди которых обязательным стандартом для OFDM является каскадный код с

внешним кодом Рида-Соломона и внутренним свёрточным кодом. Для OFDMA обязательным являются только свёрточные коды. Блок 3 осуществляет перемежение для преобразования блоков данных в последовательность, обеспечивающую возможность исправлять с помощью кодера одиночные ошибки. Схемы скремблирования в OFDM и OFDMA практически идентичны. Блок 4 осуществляет модуляцию – QAM-16, QAM-64, QPSK, BPSK. В OFDM все они являются обязательными. Для OFDMA обязательными являются QAM-16 и QPSK со скоростями кодирования½ и ¾. Квадратурная амплитудная модуляция QAM-64 является опцией. Аналогично сетям GSM, Wi-Fi и др. WiMAX предусматривает канальную адаптацию, т.е. в зависимости от качества канала используется соответствующая модуляция и схема кодирования. Оценку качества канала в WiMAX выполняют пилотные поднесущие режима OFDM, как было отмечено выше. Функция канальной адаптации выполняется на MAC-уровне. WiMAX осуществляет выбор модуляции и схемы кодирования *MCS (Modulation and Coding Scheme).*

25.3. MAC-уровень WiMAX

Структура MAC-уровня стандартов WiMAX подразделяется на три подуровня: подуровень преобразования сервиса CS (Convergence Sublayer), основной подуровень CPS (Common Part Sublayer) и подуровень безопасности (Security Sublayer). На уровне CS производится трансформация потоков данных протоколов верхних уровней (IP, Ethernet и др.) для передачи через WiMAX.

Подуровень CPS выполняет следующие функции:

- распределение полосы пропускания;
- установление соединения;
- поддержка соединения между двумя сторонами.

Подуровень безопасности выполняет между базовой станцией и абонентской станцией функции аутентификации, обмена секретными ключами, шифрования и контроль целостности.

25.3.1. Классы качества обслуживания

В стандарте мобильного доступа 802.16e-2005 предусмотрены вопросы, связные с обеспечением качества обслуживания QoS. Сервисный поток определен для обмена между базовой станцией (БС) и абонентской станцией (АС). Поскольку мобильность АС

предполагает возможность перемещения, вводится понятие “глобальный сервисный класс”. Это означает, что показатель качества обслуживания в WiMAX остается единым для всех БС. Этот глобальный сервисный класс представляет собой набор из нескольких параметров (максимальная задержка в диапазоне от 2 мс до 10с, максимальная и минимальная скорости, приоритет трафика и др.).

Кроме этого стандарт вводит понятие типов служб доставки данных, в которых приводит список нормируемых параметров, не указывая на значения. Всего предусмотрено пять типов служб доставки:

- доставка без требования, при которой нормируется максимальная задержка, минимальная гарантированная скорость передачи и другие параметры. Примером такой службы может быть VoIP [95].
- доставка в реальном времени с переменной скоростью, при которой гарантируются скорость и время задержки. Примером такой службы может быть сжатое видео по стандарту MPEG [95].
- доставка вне реального времени с переменной скоростью, при которой гарантируется минимальная скорость передачи. Примером такой службы может быть передача файлов по протоколу FTP[95].
- Доставка по мере возможности (Best Effort). Эта служба подразумевает остаточный принцип предоставления ресурса.

25.3.2. Подуровень безопасности

Задача подуровня безопасности обеспечить контроль доступа и конфиденциальность канальных данных. Это относится к аутентификации, обмену ключами и шифрованию. Алгоритм взаимодействия между базовой станцией БС и абонентской станцией АС по обеспечению ИБ построен следующим образом [96].

Защищенная связь SA (Security Association) — это блок данных, включающий параметры безопасности, которые БС и один или несколько клиентов абонентских станций согласовывают между собой для реализации безопасной связи. В этот блок данных БА входит идентификатор защищенной связи SA (16 бит), тип протокола шифрования для защиты данных в канале и два ключа шифрования данных ТЕК (Traffic encryption keys), длительность работы ключа, вектор инициализации. Один из ключей ТЕК текущий, а другой сменный. Длительность работы с одним ключом ограничена от 30 минут до 7 дней. Для работы протоколов блочного шифрования данных требуется вектор инициализации длиной

64 бит. Определено три типа данных защищенной связи: первичные (устанавливаются при инициализации связи между БС и АС), статические (устанавливаются в БС) и динамические (используется при установке соединения на транспортном уровне, когда это необходимо). Статические и динамические параметры защищенной связи могут быть установлены с несколькими мобильными станциями во время многоадресной передачи. Предоставлена возможность использовать отдельно две защищенные связи - одну для нисходящего канала, другую для восходящего канала.

Инфраструктура открытого ключа: WiMAX использует протоколы для безопасной передачи ключей между БС и мобильной станцией. Стандарт 802.16-2004 (фиксированный доступ) предусматривал аутентификацию только абонентской станции, а стандарт 802.16e-2005 (мобильный доступ) — взаимную аутентификацию. В последнем случае используется криптография с открытым ключом RSA и сертификат мобильной станции. WiMAX использует протокол EAP-TLS и сервер RADIUS (описание этого протокола приведено в главе 24) для аутентификации и контроля доступа. Функцию аутентификатора здесь выполняет БС. При успешной аутентификации в БС и АС устанавливаются общие ключи ТЕК и векторы инициализации для использования при блочного шифровании канальных данных с помощью протокола AES.

Шифрование данных: WiMAX использует протокол блочного шифрования AES для шифрования данных на участке между базовой станцией и абонентской станцией. Используя ключ шифрования и счетчик, с помощью AES создается псевдослучайная ключевая последовательность для поточного шифрования (рис. 25.2). Описание такого режима блочного шифровании приводится с использованием счетчика в приложении В. Открытый текст складывается по модулю 2 с этой ключевой последовательностью. В результате в канал от базовой станции или абонентской станции поступает зашифрованный текст в результате поточного шифрования. Этот текст из канала в абонентской станции или базовой станции складывается по модулю 2 созданной там такой же ключевой последовательностью. В результате получаем расшифрованный текст.

Рис. 25.2. Шифрование данных на радиоучастке сети WiMAX

25.4. Сети LTE

Создание конкурентной UMTS технологии WiMAX активизировало участников проекта 3GPP на создание системы мобильной связи нового поколения LTE (Long Term Evolution). В декабре 2009г. шведский оператор ввел в коммерческую эксплуатацию сеть LTE в Стокгольме (Швеция) и Осло (Норвегия). На начало 2011 года в эксплуатации находилось 18 коммерческих сетей LTE. В начале 2012 года абонентская база сетей LTE составляла 7,9 млн. в 18 странах мира [97]. По прогнозам в 2015 году абонентская база LTE будет превышать 300 млн. абонентов. По сравнению с ранее разработанными системами 3G радиоинтерфейс LTE обеспечит улучшенные технические характеристики. LTE предусмотрено для использования полосы пропускания от 1,4 до 20 МГц, что позволит удовлетворить потребности разных операторов связи, обладающих различными полосами пропускания. Оборудование LTE должно одновременно поддерживать не менее 200 активных соединений на каждую 5-МГц ячейку. LTE позволит достичь скорости до 50 Мбит/с для восходящей связи и до 100 Мбит/с для нисходящей связи. При этом должна обеспечиваться поддержка соединений для абонентов, движущихся со скоростью до 350 км/ч. Зона покрытия одной базовой станции - до 30 км, но возможна работа с ячейками радиусом более 100 км. Развитие технологии LTE проводится последовательно в рамках нескольких версий R8, R9, R10. Сформулированы основные требования, которым будет удовлетворять усовершенствованная версия 10 (LTE Advanced). По сути это требования к стандарту мобильных сетей четвёртого поколения (4G):

- максимальная скорость передачи данных в нисходящем канале до 1Гбит/с, в восходящем — до 500 Мбит/с;
- полоса пропускания в нисходящем канале — 70 МГц, в восходящем — 40 МГц.

LTE базируется на трех основных технологиях: мультиплексирование посредством OFDM, многоантенные системы MIMO и нового поколения базовой сети SAE (System Architecture Evolution), иногда называемого EPC (Evolved Packet Core) [98].

Технология OFDM, используемая также в Wi-Fi и WiMAX, предполагает передачу широкополосного сигнала посредством независимой модуляции узкополосных поднесущих.

Техника MIMO в LTE предусматривает схемы с одной, двумя или четырьмя передающими или приёмными антеннами в различных сочетаниях. В MIMO-системах возможно два вида передачи:

- каждый антенный канал транслирует независимый информационный поток (что увеличивает скорость передачи) и таких потоков может быть только два;
- передача производится параллельно по всем антенным каналам одного и того же потока (что предназначено для борьбы с помехами, что повышает качество передачи).

Сеть LTE состоит из нового поколения *сети радиодоступа E-UTRAN* (Evolved UTRAN) и *базовой сети SAE*, построенной на коммутации пакетов (рис. 25.3). Базовая сеть SAE состоит из элемента управления мобильностью MME (Moblity Management Entity) и элемента плоскости пользователя UPE (User Plane Entity). Отметим некоторые отличия LTE от UMTS.

E-UTRAN состоит только из усовершенствованных базовых станций eNB (evolved Node B), которые выполняют не только функции базовых станций UMTS, но и большинство функций контроллера сети UMTS. Базовые станции eNB соединены между собой по принципу «каждый с каждым».

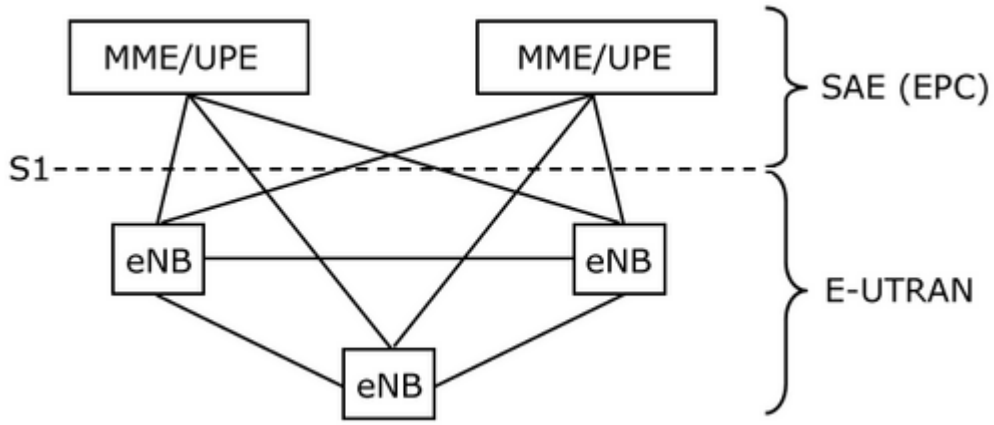


Рис. 25.3. Взаимодействие сети радиодоступа E-UTRAN и базовой сети SAE

Сетевой элемент MME отвечает за распределение сообщений вызова (paging) к базовым станциям. Сетевой элемент UPE отвечает за передачу данных пользователям. Одной из функций LTE является максимальное использование радиоресурсов, контроль и управление всеми активными сессиями передачи данных с учетом параметров качества услуг QoS. Основные требования к архитектуре сети LTE могут быть сведены к следующему:

- Поддержка сетей радиодоступа как стандартов 3GPP, так и стандартов не-3GPP. Полная совместимость с базовыми сетями стандартов 3GPP, начиная с версии R6.
- Установление IP-соединений с индивидуальными параметрами QoS.
- Функция управления мобильностью сети LTE должна решать задачи управления

мобильностью как в сети LTE, так и между сетями E-UTRAN и сетями радиодоступа других типов.

- Функция управления мобильностью сети LTE должна взаимодействовать с терминалами различных типов: фиксированными, сеансовыми (nomadic) и мобильными.
- Поддержка IP-протоколов различных версий (IPv4 и IPv6).
- Процедуры поддержки хэндовера в сетях E-UTRAN, между сетями E-UTRAN и другими сетями радиодоступа 3GPP, а также между сетями E-UTRAN/3GPP должны быть реализованы с минимальной потерей пакетов данных в режиме реального времени (например, для VoIP).
- Снижение капитальных и эксплуатационных затрат по сравнению с UMTS.
- Повышение информационной безопасности сети LTE по сравнению с UMTS. Это относится к обеспечению защиты от угроз сообщений сигнализации, к возможности смены мастер ключа и ключа шифрования во время одного установленного соединения.

При этом следует отметить продолжение в 2012 году эволюции сетей высокоскоростного пакетного доступа HSPA+ (или HSPA Evolution) [97, 98]. В сегодняшней конкурентной ситуации LTE с другими системами широкополосного доступа WiMAX и HSPA следует обратить внимание на замечание автора статьи Голышко А.В., который отметил следующие два преимущества LTE [99].

1) Увеличение спектральной эффективности по сравнению с HSPA в 3,3 раза.

2) Меньше задержка при передаче на терминал, что создает условия для более быстрой загрузки «тяжелого» контента.

В заключение по технологиям широкополосного доступа следует отметить следующее.

1. Построение сетей широкополосного доступа ШПД разных технологий (LTE, WiMAX, HSPA и др.) является одной из важных тенденций современных телекоммуникаций. Уровень использования ШПД является одним из показателей социально-экономического развития страны. В заключительном отчете комиссии по широкополосной связи для цифрового развития в 2010 году генеральному секретарю ООН говорится: «В XXI столетии сети широкополосной связи будут иметь такое же решающее значение для социального и экономического процветания, как и транспортные, электропроводные и электросети». Президент России Д.А. Медведев в своем

Послании Федеральному собранию от 12.11.2009 года заявил, что на территории всей нашей страны в течение пяти лет необходимо обеспечить широкополосный доступ в Интернет».

2. Реальные скорости передачи в ШПД часто оказываются ниже указанных в документах и рекламе. Некоторые провайдеры услуг объявляют новые тарифные планы с большими скоростями, не обеспечивая при этом реальные скорости [100].

ГЛАВА 26. Самоорганизующиеся сети SON

Одним из подходов классификации беспроводных сетей связи является деление на централизованные инфраструктуры и самоорганизующиеся. Отличительной особенностью самоорганизующихся сетей **SON (self-organization)** — это возможность в отсутствии централизованной инфраструктуры обмениваться данными любой паре находящихся в зоне радиопокрытия узлов сети. Узлы в SON могут быть одновременно конечными хостами и маршрутизаторами. Соединение организуется на длинные расстояния с помощью специализированных протоколов маршрутизации в промежуточных узлах-маршрутизаторах. Такое соединение называется «многоэтапным или многошаговым» (multihop) . Этапом является участие в этом соединении одного узла - маршрутизатора. О перспективном направлении создания в России самоорганизующихся сетей связи отмечалось заместителем директором филиала Северо-Западного филиала ОАО "Гипросвязь" д.т.н. А.Е. Кучерявым на всероссийской конференции в 2011 году «Глобальная совместимость - актуальная эадача современных телекоммуникаций» [101]. В классе SON настоящей главы рассматриваются следующие сети:

- мобильные целевые Ad Hoc сети - Wireless Mobile Ad Hoc Network (MANET);
- беспроводные сенсорные сети - Wireless Sensor Network (WSN);
- беспроводные mesh-сетей Wireless Mesh Network (WMN). Эти сети называют также *ячеистыми сетями*.
- автомобильные беспроводные сети Vehicular Ad Hoc Network (VANET).

Узлы этих сетей обладают способностью сами находить друг друга и формировать сеть, а в случае выхода из строя какого-либо узла могут устанавливать новые маршруты для передачи сообщений. В главе 24 приводится краткое описание построения самоорганизующихся сетей: MANET, ячеистой сети стандарта 802.11s, ячеистой сети WiMAX (глава 25). В настоящей главе большое внимание уделяется информационной безопасности самоорганизующихся сетей в части анализа атак «отказ в обслуживании» (DoS) в результате намеренных действий злоумышленника по нарушению работы протоколов маршрутизации. Как отмечено в работе [102], под атакой DoS понимается действие злоумышленника, приводящее к снижению способности сети выполнять возложенные на нее функции.

26.1. Функции самоорганизующихся сетей и область их использования

Структура мобильной сети Ad Hoc (MANET) приведена в главе 24. Сети MANET являются распределенной системой, состоящей из мобильных терминалов, снабженных

приемо-передатчиками. Они могут организовывать временные сетевые технологии для передачи информации. В сети MANET мобильные устройства выполняют не только функции оконечных станций, но и функции сетевых узлов (роутеров). При этом часто используется нелицензиоанная полоса частот. Приведем некоторые области применения сетей MANET.

Согласно зарубежным работам [103 и др.] наиболее широко применение мобильных сетей Ad Hoc рассматривается для установления связи во время боевых действий. При этом рассматривается установление связи между солдатами, расположенными на земле, в наземном и воздушном транспорте. Большинство узлов связи движутся с различными скоростями. Сети связи с фиксированной инфраструктурой не могут обеспечить надежную связь при таких обстоятельствах высокого темпа и высокой степени непредсказуемости. У системного администратора мало времени для того, чтобы реагировать и реконфигурировать сети. Как правило, сети MANET не требуют администрирования. Временная сеть Ad Hoc может быть развернута, когда создание инфраструктуры невозможно или неэффективно. Например, такая сеть может использоваться, как временное решение на конференциях, а также в незаселенных местах, на которых очень сложно создать инфраструктуру. Небольшое время на развертку сети Ad Hoc делает их незаменимыми при спасательных операциях после катастроф или стихийных бедствий.

26.1.1. Сенсорные сети (WSN)

Сенсорная сеть WSN — это распределенная сеть необслуживаемых миниатюрных узлов, которые осуществляют сбор данных о параметрах внешней среды и передачу их на базовую станцию посредством ретрансляции от узла к узлу с помощью беспроводной связи. Узел сети, называемый сенсором, содержит датчик, воспринимающий данные от внешней среды (собственно сенсор), микроконтроллер, память, радиопередатчик, автономный источник питания и иногда исполнительные механизмы. Возможна также передача управляющих воздействий от узлов сети к внешней среде, Сенсорные сети строятся на основе протоколов IEEE 802.15.4, ZigBee и DigiMesh. С помощью радиосвязи, осуществляемой между узлами сети на основе стандарта ZigBee, создаются самоорганизующиеся и
самовосстанавливающиеся сети. Для многих сенсорных сетей характерна мобильность не отдельно каждого узла (как это имеет место в MANET), а отдельной группы узлов. Основное требование к протоколам сенсорных сетей малое потребление энергоресурсов. В сенсорных сетях время их жизнедеятельности прямо зависит от решения вопросов энергопотребления узлов сети.

Сенсорные сети применяются в различных областях - от борьбы с терроризмом до охраны

природы. Существует множество приложений, для которых разные производители выпускают разные узлы для создания сенсорных сетей. По области применения приложения сенсорных сетей можно разделить на категории [104]:

- погода, окружающая среда;
- телемедицина;
- чрезвычайные ситуации (пожары, катастрофы и др.);
- военные операции и др.

26.1.2. Ячеистые сети (WMN)

В главе 24 приводится архитектура ячеистой сети (mesh-сети), построенной на протоколе 802.11s, принадлежащем к группе протоколов стандарта 802.11. Как отмечалось выше, mesh-сети могут быть построены на базе протоколов других стандартов- 802.16 и LTE. На рис. 26.1 приведена общая архитектура mesh-сети [105]. Как видно из рисунка mesh-сеть состоит из беспроводной опорной сети (Wireless Mesh Backbone) и поключенных к ней сети Интернет, сети Wi-Fi, сотовых сетей связи, оконечных пользователей. Непрерывной линией обозначен проводный канал, а пунктирной — беспроводный канал.

Беспроводная опорная сеть (Wireless Mesh Backbone) включает следующие маршрутизаторы:

- mesh-роутер без шлюза (Mesh Router).
- mesh-роутер с шлюзом (Mesh Router with Gateway), взаимодействующий с Интернетом и остальными типами mesh-роутеров.
- mesh-роутер с шлюзом и мостом (Mesh Router with Gateway/Bridge), взаимодействующим со всеми mesh-роутерами опорной сети, а также точкой доступа сети WiMAX, базовыми станциями сотовой сети связи и сети WiMAX. узлом сенсорной сети связи (Sink Node), непосредственно с абонентами по проводному или беспроводному каналу.

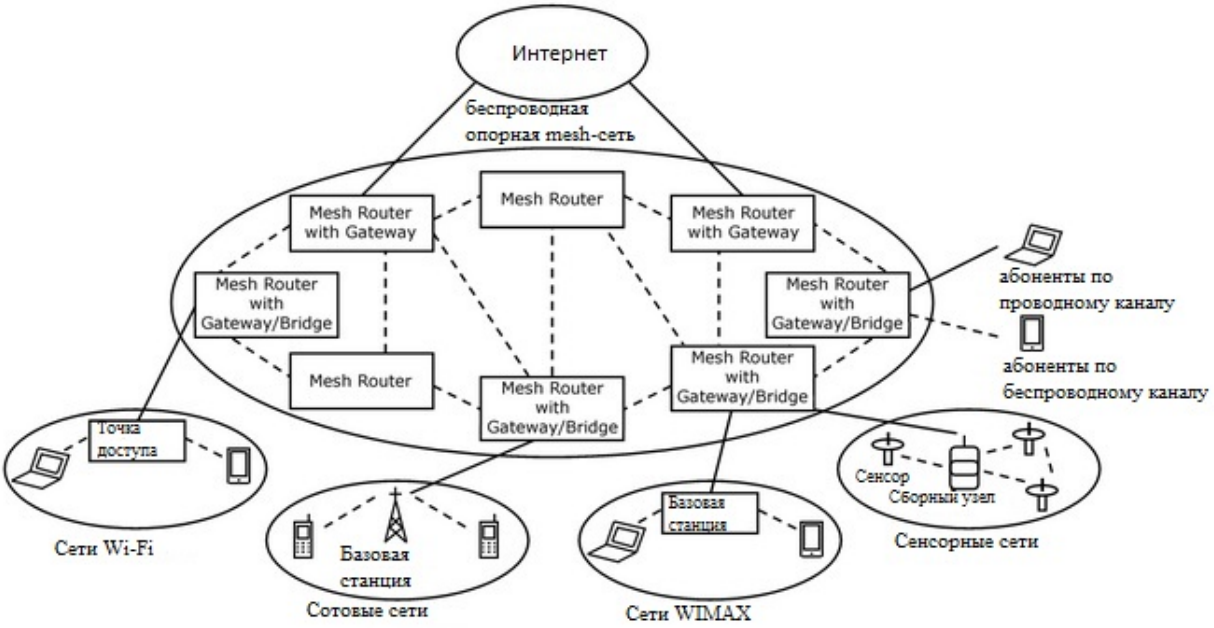


Рис. 26.1. Архитектура mesh-сети

В работе [105] приводится ещё одна архитектура mesh-сети, позволяющая абонентам дополнительно обеспечивать не только доступ в Интернет, но и связь между собой внутри опорной сети. Сравнивая с MANET и сенсорными сетями, ячеистые беспроводные сети отличаются по следующим четырем признакам:

- Роутеры в ячеистых сетях способны пропускать больше трафик и имеют меньше ограничений в плане энергозатрат.
- Сети маршутизаторов могут обеспечить передачу данных на более дальние расстояния.
- Сети маршрутизаторов могут быть использованы в качестве интегратора таких сетей, как Интернет, сотовые сети, беспроводные локальные сети.
- В ячеистых сетях любой роутер имеет, по крайней мере, два радиоканала: один для подключения клиентов, другой для связи с другими роутерами.

Почти любое применение мобильных Ad Hoc сетей, рассмотренное выше, может быть реализовано в беспроводных ячеистых сетях. Основным достоинством ячеистых сетей является способность передавать большие объемы данных на дальние расстояния и обеспечение широкополосного доступа.

26.1.3. Автомобильные беспроводные сети (VANET)

Создание автомобильных беспроводных самоорганизующихся сетей VANET предназначено для повышения эффективности и безопасности дорожного движения. В

настоящее время при поддержке индустрии, государственных и академических институтов в мире выполняются несколько научно-исследовательских проектов, направленных на разработку и принятие стандартов таких автомобильных сетей. Основные цели использования VANET можно разделить на три группы [93]:

- помощь водителю (навигация, предотвращение столкновений и смена полос);
- информирование (об ограничении скорости или зоне ремонтных работ);
- предупреждение (послеаварийные, о препятствиях или состоянии дорог).

26.2. Угрозы безопасности самоорганизующихся сетей

Перечислим причины уязвимости информационной безопасности самоорганизующихся сетей:

- Уязвимость каналов к прослушиванию и подмене сообщений по причине общей доступностью среды передачи, как и в любых беспроводных сетях.
- Незащищенность узлов от злоумышленника, который легко может изъять из сети (обычно находятся в открытых местах) и использовать их в своих целях.
- Отсутствие инфраструктуры делает классические системы безопасности, такие как центры сертификации и центральные серверы, неприменимыми.
- Динамически изменяющаяся топология сети требует использования сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов в результате изменения топологии сети.
- Подходы к обеспечению информационной безопасности в мобильных самоорганизующихся сетях значительно отличаются от подходов к реализации ИБ в проводных сетях ввиду самой природы радиоканала. Связь осуществляется через беспроводную среду, таким образом, передаваемые и получаемые сигналы передаются через воздух. Следовательно, любой узел, находящийся в диапазоне источника сигнала, знающий частоту передачи и другие физические параметры (модуляцию, алгоритм кодировки) потенциально может перехватить и раскодировать сигнал. Причем ни источник сигнала, ни получатель не будут об этом знать. В проводной сети, наоборот, такой перехват будет возможен, если злоумышленник физически будет иметь доступ к проводному каналу, что на практике гораздо сложнее.
- В централизованных сетях злоумышленники могут анализировать трафик или всю систему на предмет подозрительного поведения и в случае необходимости выполнять определенную политику безопасности. Подобный механизм невозможно реализовать в

Ad Hoc, так как каждый узел в таких сетях имеет столько же привилегий, как и все остальные. Кроме того, как было сказано выше, эти сети не имеют четкой топологии, а напротив, каждый узел может свободно перемещаться.

Подводя итог, можно отметить, что самоорганизующуиеся сети Ad Hoc уязвимы к классическим типам атак, присущим всем беспроводным сетям, так и имеют свои особенности. Ввиду того, что беспроводные самоорганизующиеся сети не имеют фиксированной топологии, центральных узлов, стабильных источников питания, широкополосного канала, постоянной связи узлов задача злоумышленника по реализации успешной атаки становится легче выполнимой. Атаки на информационную безопасность в самоорганизующихся сетях делятся на пассивные и активные. В пассивных атаках злоумышленник обычно скрыт. Он подсоединяется к линиям связи для того, чтобы собирать данные. Пассивные атаки могут быть сгруппированы и разбиты на два класса: перехват (сниффинг) и анализ трафика.

26.2.1. Перехват

Передаваемые данные могут быть перехвачены путем подслушивания линий передач (радиокаланала). Стоит отметить, что беспроводные линии связи легче подслушать ввиду самой природы радиоканала. Поэтому беспроводные сети более уязвимы для пассивных атак.

26.2.2. Анализ трафика

Точно так же, как и содержание пересылаемых пакетов, вид (характер) трафика может дать много информации злоумышленнику. Например, анализируя трафик можно извлечь важную информацию относительно топологии сети, маршрутизации. По результатам анализа трафика злоумышленник может провести активную атаку и уничтожить некоторое количество узлов, что вызовет переконфигурацию сети и пересылку ценной информации от узла к узлу. В этом случае можно собрать информацию о топологии сети.

В активных атаках злоумышленник влияет на операции, происходящие в атакуемой сети. Это воздействие может быть целью атаки и, как правило, может быть обнаружено. Активные атаки могут быть классифицированы на следующие группы.

- Физические.
- Фальсификация (спуфинг), повтор и изменение сообщений.
- Отказ в обслуживании.

26.2.3. Физические атаки

Злоумышленник может физически разрушить используемое оборудование, чтобы уничтожить узел. Физические атаки, нацеленные на оборудование, могут быть серьезной проблемой, особенно в военной связи. Другим типом физической атаки является электромагнитный импульс (ЭМИ). ЭМИ - это непродолжительный по времени выброс электромагнитной энергии, который может вызывать временный всплеск напряжения во всех электронных устройствах, что может привести к их поломке. ЭМИ есть обычный результат ядерных взрывов. На сегодняшний момент даже доступны переносимые устройства, которые способны вызывать ЭМИ. Несмотря на то, что использование ЭМИ до сих пор не всегда является целесообразным, эта технология представляет угрозу для всех электронных устройств, находящихся в пределах тактической зоны.

26.2.4. Фальсификация, повтор и изменение сообщений

Фальсифицированный узел ведет себя, как другой, санкционированный узел. Эти узлы могут перехватывать сообщения, сохранять и пересылать дальше (повтор). Наконец, содержимое перехваченных сообщений может быть изменено до того, как оно будет доставлено адресату. В результате могут быть реализованы различные сценарии атак. В мобильных самоорганизующихся сетях узлы могут произвольно менять свое положение в пространстве. Реализация спуфинга в них представляется более легкой, чем в других типах сетей. Механизмы самоорганизации сети работают таким образом, чтобы уметь приспособиться к изменениям в топологии. Поскольку протоколы маршрутизации могут не иметь четкой картины сети, мы можем не знать, присоединился ли какой-либо узел к сети или нет. А если и присоединился, то не сделал ли он это дважды, в разных точках сети. В сенсорных сетях фальсификация еще более вероятна, т.к. эти сети могут не использовать какую-либо повсеместную систему идентификации. Сенсорные сети, в частности, имеют несколько больше функций, которые наиболее чувствительны к таким типам атак, т.к. одной из главных особенностей сенсорных сетей является работа, основанная на коллективном сборе данных многих узлов.

Такие атаки, как фальсификация, повтор и изменение сообщений могут быть направлены против конфиденциальности данных. Сфальсифицированные узлы могут заставлять другие узлы пересылать им конфиденциальные данные. Они также могут использоваться для того, чтобы получить неавторизированный доступ к системным ресурсам. Узел, который выдает себя за другой узел, может обманом вызвать пароли и логины для доступа к конфиденциальной информации, причем она ему будет передана

добровольно, т.к. санкционированный узел будет принимать его за достоверного участника сети.

26.2.5. Атаки DoS (“ отказ в обслуживании”)

Атака в сети типа “отказ в обслуживании” DoS-атака определяется как любое событие, которое угрожает способности сети выполнять правильно в определенный промежуток времени свои обычные функции. DoS-атака характеризуется следующими последствиями при реализации целей злоумышленником: снизить качество обслуживания сетью или вовсе не дать сети выполнять свои обычные функции. Почти каждый сетевой сервис может быть целью DoS-атаки. Рассмотрим основные сценарии DoS-атак на нижних уровнях транспортной сети связи. При этом основное внимание уделим анализу атакам злоумышленника, нарушающим маршрутизацию и, как следствие нарушающим работу сети.

26.2.5.1. DoS на физическом уровне

Все физические атаки, описанные выше, могут быть также классифицированы, как DoS-атаки ввиду того, что они мешают сети выполнять свои регулярные функции. В этом разделе, под физическим уровнем мы будем понимать физический уровень модели OSI, который ответственен за представление 0 и 1 в беспроводной среде. DoS-атака на этом уровне называется зашумление (jumming).

Неприятельское устройство может «забивать» полезный сигнал внутри сети, передавая свой зловредный сигнал на той же частоте. Этот сигнал будет добавлять шум к несущему полезному сигналу, ослабляя его силу и увеличивать помеху. Таким образом, соотношение сигнал/шум в несущем сигнале будет меньше, чем нужно узлам сети для правильного приема. Затор может проводиться непрерывно в какой-либо области, что мешает всем узлам этой области правильно принимать сигнал.

26.2.5.2. DoS на канальном уровне

Алгоритмы канального уровня, особенно алгоритмы получения доступа к среде (MAC) являются сильно уязвимыми для DoS-атак. В самоорганизующихся сетях используются протоколы множественного доступа с контролем несущей и предотвращением коллизий CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Один из них (протокол MACAW), использующий последовательность сообщений RTS-CTS-DATA-ACK, приведен для сети MANET в главе 24. Например, DoS-атака MAC уровня может надолго прерывать работу канала следующим образом, воздействуя на такой механизм.

- Когда получен RTS, можно посылать сигнал, который будет вступать в коллизию с

CTS. Поскольку узлы не могут начать передачу до того, как будет получен CTS, они будут продолжать посылать RTS.

- Если MAC протокол основан на наличии спящих и активных периодах, то глушение только активных периодов может продолжительно блокировать канал.
- Если заведомо ложные RTS и CTS сигналы с несоизмеримо большими параметрами длительности передачи будут непрерывно посылаться в сеть, то другие узлы могут ждать своей очереди недопустимо очень долго.

26.2.5.3. DoS маршрутизации

Для самоорганизующихся сетей характерны также потенциальные угрозы, реализующиеся в виде DoS-атак, направленных на нарушение легитимной работы маршрутизации. Все такие атаки можно условно разделить на два типа: атаки нарушения маршрутизации и атаки потребления ресурсов. Первый тип атак направлен на то, чтобы заставить протокол маршрутизации работать неправильно, перестать выполнять необходимые функции. У атак потребления ресурсов цель другая. Она заключается как можно в большем потреблении ресурсов сети, таких как пропускная способность, канала, память, вычислительные способности и электроэнергия. Оба этих типа атак относятся к DoS-атакам. Примеры таких атак и их краткое описание приведены ниже.

- Сфальсифицированная (spoofed), измененная (altered) или нелегитимно повторенная (replayed) информация о маршрутизации: сообщения, которыми обмениваются узлы, могут быть таким образом изменены злоумышленниками, что приводит к нарушению маршрутизации сети.
- Атака затопления «Hello» (hello flood attack): нарушающий узел передает широковещательную или другую информацию достаточно мощным сигналом, показывая каждому узлу в сети, что он является их соседом (рис. 26.2). Когда другие узлы передают свои пакеты настоящим соседним узлам, то они не принимаются ими.

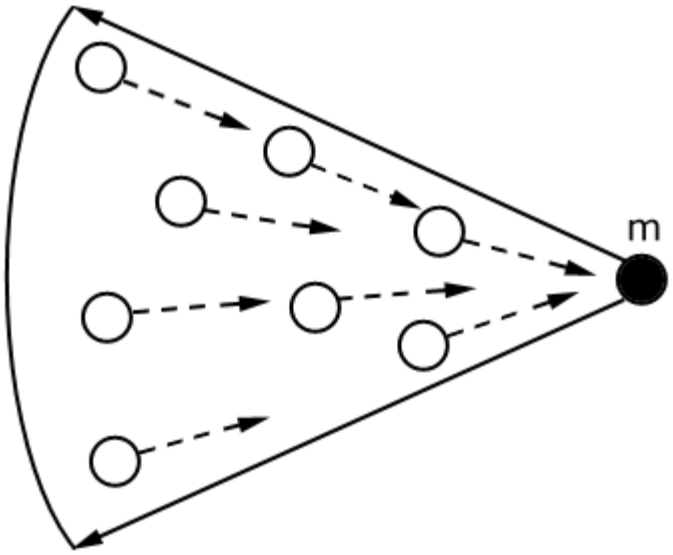


Рис. 26.2. Атака затопления «Hello»

- Атака типа «червоточина» (wormhole attack): нарушающий узел может перехватывать пакеты в какой-либо точке и пересылать их другому нарушающему узлу, который находится в другой части сети. Причем эта передача будет происходить вне полосы канала. Второй узел затем будет повторять передачу пакетов. Все узлы, которые будут способны услышать повторную передачу второго злоумышленного узла, будут считать, что узел, который послал пакеты первому злонамеренному узлу, является их близким соседом. На рис. 26.3. приведен пример такой атаки. Узел a передает пакеты. Эти пакеты получают узлы b и w1. Причем, b является санкционированным, а w1 злоумышленным. Затем w1 переправляет пакет другому несанкционированному узлу w2 по каналу, который недоступен другим узлам сети, кроме враждебных. Узел w2 повторяет пересылку пакета, который доходит до узла f. Пакеты, которые следуют по обычному пути, т.е. a-b-c-d-e-f, достигают узла f позже, чем те, которые были переданы по червоточине. Таким образом, пакеты, которые пришли с задержкой, будут отброшены ввиду того, что имеют больше количество пройденных на маршруте узлов (хопов, hops). Атаки типа червоточина очень сложно обнаружить. Они могут влиять на производительность многих сетевых сервисов таких как: синхронизация во времени, локализация или синхронизация данных.

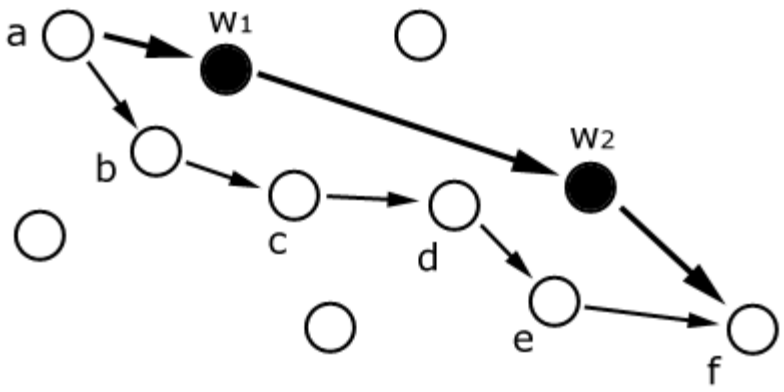


Рис. 26.3. Атака типа «червоточина»

- Обход (detour attack): атакующий может попытаться направить трафик в обход основного пути, по пути менее оптимальному или вообще по другой части сети. Для этого могут применяться различные способы. Например, существует атака типа «даровой обход», где враждебный узел располагает виртуальные узлы на основном пути. Таким образом, правильный путь становится дороже с точки зрения числа хопов и трафик идет в обход по пути, который выгоден злоумышленнику.
- Сборный пункт (sink hole attack): нарушающий узел может быть с точки зрения алгоритма маршрутизации наиболее оптимальным для всех окружающих узлов. Например, нарушающий узел может рассылать сообщения маршрутизации, убеждая все соседние узлы, что он является наилучшим узлом для последующей передачи пакета на базовую станцию. Это позволяет ему стать концентратором и собирать все пакеты от всех узлов его окрестности, идущие к базовой станции. Это открывает большие возможности для последующих типов атак.
- Черная дыра (black hole attack): нарушающий узел может уничтожать все пакеты, которые он получает для последующей передачи. Этот тип атаки особенно эффективен, когда узел является одновременно сборным пунктом. Такая комбинация может быть причиной останова передачи большого объема данных.
- Выборочная пересылка (серая дыра - gray hole attack, selective forwarding): когда нарушающий узел уничтожает все получаемые пакеты, это может быть легко обнаружено соседними узлами. Поэтому нарушитель может уничтожать пакеты данных выборочно, а остальные транслировать правильно.
- Атака Сибиллы (Sybil attack): один узел представляет собой несколько узлов для других участников сети. Это является большой проблемой для протоколов маршрутизации. Кроме того, это может влиять на другие сервисы сети, такие как

вычисление аномального поведения, алгоритмов, основанных на голосовании, собирании и соотнесении данных и распределенном хранении информации.

- Зацикливание (routing loop attack): атаки типа обход и сборный пункт могут использоваться для создания зацикливания для того, чтобы потреблять энергию и пропускную способность, а также для того, чтобы препятствовать правильной маршрутизации.
- Rush-атака: атакующий очень распространяет сообщения о запросе путей маршрута и быстро повторяет эти сообщения по всей сети. Это создает затор другим легальным запросам путей маршрута.
- Атаки, использующие схемы обхода неработающих узлов: в некоторых алгоритмах маршрутизации существуют техники, которые позволяют избегать использования узлов с низкими показателями производительности или энергообеспечения для того, чтобы иметь больше шансов на доставку пакета. Такие схемы могут быть использованы злоумышленниками. Например, враждебный узел может посылать сообщение об ошибки для узла, который на самом деле работает хорошо. Ввиду этого, протокол маршрутизации будет стараться избегать использования этого узла для последующей передачи пакета. Другим примером является зашумление какой-то конкретной связи на короткий временной интервал. За этот интервал будет сгенерировано сообщение об ошибке, и протокол маршрутизации будут стараться искать обходной путь даже, если эта связь уже не является зашумленной.
- Атаки, направленные на истощение сетевых ресурсов (attacks to deplete network resources): когда узлы не являются постоянно обслуживаемыми и полагаются только на свои имеющие ограничения ресурсы, злоумышленник может попытаться их истощить, чтобы подорвать работу сети. Для сенсорных сетей такой вид атак несет большие последствия в отношении истощения источников питания узлов. Стандартным методом реализации этой атаки является отправка фиктивных пакетов, обязательных для обработки.

26.3. Протоколы маршрутизации

Настоящий раздел посвящен изложению общих положений по алгоритмам маршрутизации в самоорганизующихся сетях. Отдельное внимание этому мы уделяем здесь в связи с высокой их чувствительностью к атакам DoS.

Для сетей Ad Hoc не подходит использовать протоколы маршрутизации сетевого уровня в TCP/IP сетях, хотя в них и предусмотрена адаптивность к изменениям топологии сети.

Однако в сетях Ad Hoc изменения могут происходить очень часто, что может привести к частой передаче информации об изменении топологии. С ростом сети это приводит к большому расходу частотных, вычислительных и энергетических ресурсов [106]. Протокол маршрутизации в сети Ad Hoc должен быть легко адаптирован к изменениям сетевой топологии при перемещении мобильных устройств (роутеров, терминалов), оптимальным с точки зрения использования сетевых ресурсов, масштабируемым. Исходя из этого, в Ad Hoc требования к протоколам маршрутизации ужесточаются. Разработано более 30-ти протоколов маршрутизации Ad Hoc.

26.3.1. Протоколы маршрутизации сети MANET

В соответствии со стратегией роутеров протоколы маршрутизации могут быть разделены на протоколы управляемые таблицами (table-driven) и протоколы маршрутизации по требованию (on-demand). Протоколы, управляемые таблицами, называются также проактивными, так как они собирают информацию о топологии сети до того, как передача будет инициализирована. Каждый узел в сети содержит таблицу маршрутизации, которая, в свою очередь, содержит всю необходимую информацию о пути до любого другого узла в сети. Эта информация содержится в специальных таблицах, которые периодически обновляются по мере того, как топология сети меняется или с определенным интервалом времени. Многие протоколы из этой категории были созданы на основе классических протоколов маршрутизации сетей TCP/IP. Существуют небольшие различия между протоколами в этой категории, в зависимости от того, какая информация содержится в таблицах маршрутизации. Более того, различные протоколы хранят и обновляют разное количество таблиц. Проактивные протоколы не подходят для больших сетей, так как они требуют наличия информации о каждом узле в сети. Протоколы маршрутизации по требованию называются также реактивными, поскольку они не обладают информацией о возможных путях до инициализации соединения. Таблицы маршрутизации не поддерживаются, обновления их не требуется. Если один узел желает послать пакет другому узлу, протокол маршрутизации реактивный будет искать возможный путь по требованию и установит соединение после того, как найдет получателя. Важной задачей реактивного протокола является поддержание установленного маршрута, поскольку велика вероятность разрыва соединения. По сравнению с проактивными протоколами реактивные обладают меньшей избыточностью и большей масштабируемостью. Однако при использовании реактивных протоколов возможны значительные задержки в передаче данных, поскольку перед самой передачей данных происходит поиск нужного маршрута. К данной категории относится протокол AODV.

26.3.1.1. Требования к протоколам маршрутизации в MANET

Поскольку в самоорганизующейся сети отсутствует фиксированная инфраструктура, узлы сети являются одновременно и мобильными терминалами и маршрутизаторами. Маршрутизация в самоорганизующихся пакетных радиосетях является сложной задачей. Она существенно отличается от традиционной маршрутизации в проводных сетях. Связь между узлами по радиоканалу часто является прерывистой, эпизодической и не может быть гарантирована. Из-за подвижности узлов и самопроизвольной организации соединений топология сети претерпевает частые, непредсказуемые и значительные изменения. Дальность радиосвязи в сети ограничена, непосредственная связь между многими парами узлов невозможна. В связи с этим необходимо использование маршрутизации с множественными переходами, скачками. При такой маршрутизации пакет передается от одного узла другому, пока не достигнет получателя. Протоколы маршрутизации самоорганизующихся пакетных радиосетей должны обладать следующими свойствами.

Распределенность. Протокол маршрутизации не должен зависеть от некоторого центрального узла, поскольку узлы могут достаточно часто покидать сеть и присоединяться к ней. Из-за подвижности узлов сеть может оказаться разделенной.

Отсутствие петель. Отсутствие в маршруте петел позволяет избежать избыточной загрузки канала, перегрузки процессоров узлов, уменьшить время доставки, уменьшить энергопотребление мобильного устройства.

Операции по запросу. Реактивные протоколы маршрутизации, устанавливающие маршрут по запросу, позволяют уменьшить объем передаваемой служебной информации и, соответственно, более эффективно используют ресурсы сети.

Поддержка однонаправленных каналов. Как правило, протоколы маршрутизации рассчитаны на работу с двунаправленными соединениями. Однако в самоорганизующихся сетях весьма часто могут устанавливаться однонаправленные соединения по следующим причинам:

- различие характеристик оборудования соседних узлов, таких как мощность передатчика и чувствительность приемника;
- интерференция - помехи рядом с узлом А могут позволять ему принимать пакеты от узла В, в то время как узел В может находиться в зоне действия более сильных помех;
- условия чрезвычайных ситуаций, когда узел работает только на прием.

Использование однонаправленных соединений способствует увеличению общей

производительности системы.

Энергосбережение. Поскольку емкость батареи мобильных узлов ограничена, необходимо рационально ее использовать. Для экономии заряда батареи узлы должны находиться максимальное время в спящем режиме. Протокол маршрутизации должен обеспечивать эффективность при минимальном задействовании узлов.

Организация нескольких маршрутов. Для предотвращения потери пакетов из-за разрыва соединений и перегрузки канала можно использовать запасные маршруты. При выходе из строя одного маршрута другой остается доступным, и нет необходимости заново проводить поиск и организацию маршрута.

Обеспечение QoS. QoS должно обеспечиваться на всех уровнях стека протоколов сети. Для многих протоколов маршрутизации существуют свои расширения, обеспечивающие QoS. Например, у протокола AODV это расширение называется QoS-AODV.

26.3.1.2. Протоколы маршрутизации AODV и SAODV

Уязвимость радиоканалов и узлов, отсутствие фиксированной инфраструктуры и частые изменения топологии сети делают неприменимыми для самоорганизующихся сетей многие известные решения по защите от атак DoS маршрутизации. Ниже рассматривается один из таких эффективных протоколов маршрутизации, который принадлежит семейству реактивных протоколов [104]. Название этого протокола Ad Hoc on demand distance vector protocol (AODV), что переводится на русский язык как протокол маршрутизации по требованию на основе вектора расстояний. Протокол AODV специально разработан для MANET. В AODV узел, желающий переслать пакет узлу, к которому он еще не имеет пути в своей таблице маршрутизации, будет пытаться найти путь. Нахождение нового пути происходит с помощью рассылки по всей сети сообщения о запросе пути, которое называется RREQ (route request message). Таким образом, узел, желающий передать пакет другому узлу, посылает сообщение RREQ. Сообщение RREQ содержит IP-адрес отправителя и IP-адрес получателя сообщения, т.е. узла, с которым необходимо установить связь отправителю. RREQ распространяется по всей сети до того момента, когда найдется узел, знающий путь до получателя или найдется сам получатель. В этом случае в ответ будет послано сообщение о том, что путь найден. Это сообщение называется RREP (route reply message). RREP посылается обратным путем к отправителю. Во время обратной отсылки RREP устанавливается связь. В RREQ существует еще одно поле, которое называется время жизни (time to live) или TTL. Это поле устанавливается отправителем для того, чтобы иметь возможность определить и ограничить глубину путешествия пакета RREQ перед тем, как он

найдет получателя. Таким образом, RREQ будет распространятся по сети до тех пор, пока количество уже посещенных пакетом узлов будет меньше, чем TTL.

Одно из полей этого сообщения называется количество посещенных узлов (hop-count field). Оно сообщает о количестве узлов посещенных пакетов до того, как он достиг текущего узла. В тот момент, когда узел получает RREQ, он проверяет количество уже посещенных узлов до того момента, как сообщение достигло его (hop count field). Затем он создает новый путь до отправителя RREQ сообщения (если только он не имеет уже более короткий путь) для того, чтобы иметь возможность использовать его для отправки RREP сообщения. Причем путь до отправителя от этого узла будет идти через узел, от которого было получено сообщение RREQ. Длина пути будет равна числу, содержащемуся в поле hop-count field полученного RREQ. Затем узел проверяет, знает ли он путь до получателя, IP-адрес которого содержится в RREQ.

Если узел, принявший RREQ, не знает путь до получателя, он увеличивает число в hop count field и переправляет RREQ своим соседям. Если RREQ получено узлом, который знает свежий путь до получателя или RREQ получено самим получателем, то узел отвечает отправителю RREQ сообщением RREP. Сообщение RREP посылается только начальному отправителю RREQ по пути, который был создан во время распространения сообщения RREQ. Сообщение RREP также содержит поле (hop count field), указывающее количество узлов от узла, сгенерировавшего RREP до получателя (причем 0 будет, если RREP генерируется самим получателем).

Это поле также увеличивается на один каждым узлом, переправляющим RREP по пути от получателя к отправителю. Поскольку каждый узел, который знает свежий путь к получателю, будет генерировать RREP, то к отправителю придет несколько сообщений RREP, которые будут указывать путь к получателю. Когда отправитель RREQ сообщения получает много RREP, он может сравнить их по полю hop count field, которое будет свидетельствовать о длине пути. Выбранным будет путь с наименьшим значением в hop count field. Опционно, отправитель RREQ сообщения может также посылать пакет, подтверждающий прием сообщения RREP, который называется RREP-ACK.

На рис. 26.4 показана работа протокола AODV. На этом рисунке отправитель A желает найти путь к получателю B. Узел A создает и распространяет сообщение RREQ. Узел B отвечает сообщением RREP после получения RREQ, используя уже созданный путь. Необходимость защиты протокола AODV от приведенных выше атак DoS нарушения маршрутизации потребовал его модифицировать. Этот протокол получил название

безопасного протокола SAODV (Secure AODV). Он обеспечивает подлинность источника сообщений RREQ и RREP, целостность этих сообщений. В SAODV для этого предусмотрены механизмы цифровой подписи и хеш-цепей. Механизм цифровой подписи служит для защиты неизменяемых полей в сообщениях между узлами сети. Сообщения RREQ и RREP также содержат переменную информацию, которая должна изменяться после каждого узла. Это поле не подписывается отправителем служебного сообщения. Второй механизм (хеш-цепи) используется для защиты такой изменяемой информации, в качестве которой является счетчик скачков (хопов).

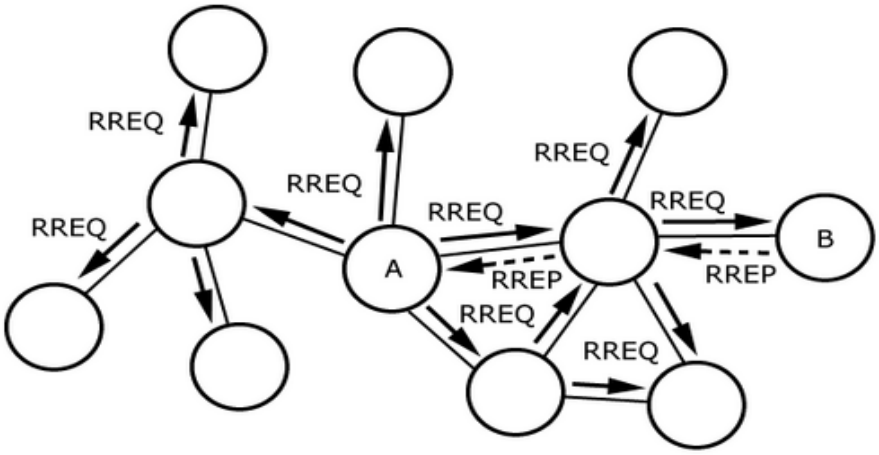


Рис. 26.4. Иллюстрация работы протокола AODV

26.3.2. Протоколы маршрутизации беспроводной сенсорной сети

Существующие протоколы маршрутизации сетей MANET не могут быть использованы в беспроводных сенсорных сетях WSN по причине следующих особенностей функционирования WSN [103].

- Ограничение потребления энергии. Сенсор в силу своего малого размера может быть оборудован только источником питания ограниченного размером. В определенных приложениях сенсорных сетей, например решение тактических задач в тылу врага, сенсор является необслуживаемым устройством и замена источника питания в нем невозможна. Особое внимание в протоколах маршутизации сенсорных сетей уделяется снижению частоты передачи/приема информации.
- Ограниченная масштабируемость. Повышение количества сенсоров в сети может привести к перегрузке маршрутных таблиц, блокировке сенсоров и, соответственно, выходу из строя сети.

На рис. 26.5 приведены диаграммы для иллюстрации одного из таких протоколов маршутизации в сенсорных сетях-SPIN (Sensor Protocols for Information via Neotivation). SPIN относится к адаптивным протоколам, в котором для болеее экономичного потребления электроэнергии первоначально отправляются не полные данные, а только их основные характеристики. Полные данные передаются при их затребовании. SPIN использует три типа сообщений: ADV, REQ и DATA. Прежде, чем отправить сообщение DATA сенсор отправляет широковещательно сообщение ADV, содержащее краткое описание полного сообщения DATA. Если соседний узел заинтересован в получении DATA, он отправляет в ответ запрос REQ на него. После получения DATA этот соседний узел повторяет, как показано на рис. 5, предоставляя другим узлам получить копии сообщения DATA.

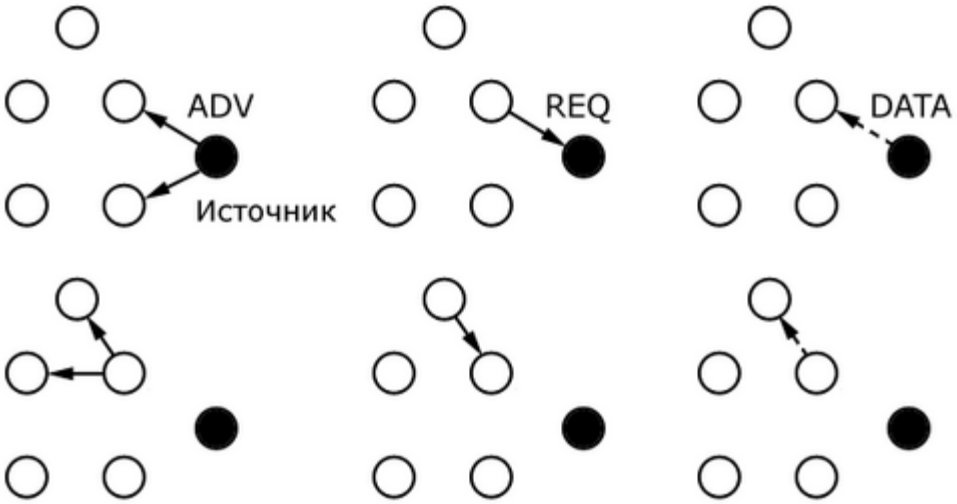


Рис. 26.5. Диаграмма протокола маршутизации в сенсорных сетях SPIN

При этом следует отметить, что в сенсорных сетях возможности по защите от атак DoS нарушения маршрутизации значительно меньше, чем в сетях MANET. В частности, это относится к ограничениям не только энергопотребления, но и аппаратным ограничениям (объем памяти порядка нескольких Кбайт, длина пакета порядка 30 байт). В результате в сенсорных сетях представляется практически сложно реализовать такие механизмы, как асимметричную криптографию, шифрование по алгоритму AES. Поэтому для сенсорных сетей разработаны два протокола безопасности [107]: протокол шифрования SNEP (sensor network encryption protocol) и протокол μTESLA. SNEPобеспечивает конфиденциальность данных, аутентификацию двух участников обмена данными, целостность данных и защиту от повтора. μTESLA обеспечивает аутентификацию для широковещательных сообщений.

26.3.3. Протоколы защиты маршрутизации mesh-сети

Для того чтобы рассмотреть безопасность протоколов маршрутизации mesh-сети следует учесть, что в общем случае эту сеть можно рассматривать из инфраструктурной части и сети Ad Hoc. В качестве инфраструктурной части может быть сотовая сеть связи, IP-сеть, Wi-Fi в режиме инфраструктуры. В этих сетях отсутствуют проблемы безопасности протоколов маршрутизации. В самоорганизующихся сетях Ad Hoc защита протоколов маршрутизации аналогична тем, которые имеют место в сетях MANET [108]. Выше, в разделе 26.3.1 приводится пример такого безопасного протокола SAODV, который обеспечивает подлинность источника сообщений маршрутизации и их целостность.

26.3.4. Безопасность автомобильной беспроводной сети (VANET)

В апреле 2010 года был утвержден новый стандарт IEEE 802.11p для связи между машинами и дорожной инфраструктурой, а также для связи непосредственно между автомобилями, движущимися со скоростями до 200 км/час на расстоянии до 1000 м. Физический и MAC-уровни основаны на IEEE 802.11a. Хотя VANET является одной из форм MANET, однако некоторые различия не предоставляют возможность использовать протоколы маршрутизации MANET. Причиной является характерная для VANET высокая динамическая природа сети, частая смена топологии сети, непостоянные пользователи сетью и кратковременные связи [108] . Другая особенность VANET заключается в большом числе взаимодействующих объектов в течение короткого времени. Автомобиль может устанавливать соединения с тысячами других автомобилей в зависимости от трафика, скорости и трассы.

Стандарт 802.11p учитывает эту специфику и как она отражается на возможных угрозах информационной безопасности сети. Это относится и к атакам злоумышленника на сетевом уровне с помощью фальшивых сообщений, нарушающих маршрутизацию. Главное преимущество этого стандарта — дешевизна, обусловленная большими объемами производства, что делает внедрение более легким и ускоряет вхождение на рынок [109]. Приведем некоторые из требований к информационной безопасности, сформулированные в работе [110].

- Аутентификация является главным требованием к ИБ в VANET. Это вызвано необходимостью защиты от различных сообщений, отправленных от несуществующих узлов (например, атака Сибиллы) или от узлов, выдающих себя за существующие. Атака может быть и от реального узла, когда водитель направляет фальшивое сообщение о пробке на дороге для освобождения себе пути проезда.
- Целостность сообщений, гарантирующая от приема фальшивых сообщений.
- Обеспечение невозможности отказа отправителя от переданных им сообщений.
- Контроль доступа позволяет гарантировать, что все узлы функционируют в соответствии с предоставленными им полномочиями и привилегиями.
- Конфиденциальность сообщений в случаях, связанных с подозрениями в криминале.
- Обеспечение защиты приватной информации пользователя.

ПРИЛОЖЕНИЕ А. Общие положения безопасности сетей связи

Настоящее приложение состоит из трех частей: задачи безопасности сетей связи, архитектура безопасности сетей связи и метод количественной оценки угрозы безопасности сети связи. В них приводятся общие положения безопасности сетей связи, изложенные в стандартах международного союза электросвязи ITU-T (рекомендации E.408 и X.805).

А.1. Задачи безопасности сетей связи

Ниже приведены задачи информационной безопасности в сетях связи, сформулированные в рекомендации ITU-T E.408 [111].

- Только допустимый участник электросвязи ТА (Telecommunication Actor) должен иметь возможность доступа к сети связи и пользоваться ею. К участнику связи ТА относятся: оператор сети, поставщик услуг, конечный пользователь услугами сети, продавец аппаратного/программного обеспечения, третий доверенный участник.
- ТА должен иметь легитимный доступ к ресурсам. Под термином «доступ к ресурсам», следует понимать возможность не только выполнять функции, но и читать информацию.
- Сети связи должны обеспечивать секретность на уровне, определенном политикой безопасности в данной сети.
- ТА должен нести ответственность за свои и только свои действия в сетях связи.
- Чтобы обеспечить доступность, сети связи должны быть защищены от непредусмотренного доступа или действия.
- Должна быть обеспечена возможность получения от сетей связи информации, относящейся к безопасности (но только легитимные ТА должны иметь возможность запросить такую информацию).
- При обнаружении нарушения безопасности необходима обработка таким образом, чтобы минимизировать потенциальный ущерб.
- При обнаружении взлома безопасности должна существовать возможность восстановления нормальных уровней безопасности.
- Архитектура безопасности сетей связи должна обеспечить поддержку разных стратегий безопасности, например различную эффективность механизмов безопасности.

К перечисленным выше задачам относятся также ограничения, которые налагаются

государственными законами и директивами. Эти ограничения могут включать обязательные услуги безопасности (такие как гарантии секретности приватной информации о клиенте), гарантии не разглашать информацию о прослушивании правоохранительными органами и содержания прослушиваемой информации.

Угрозы – это потенциальное нарушение безопасности. Каждая угроза означает риск. Оценка риска может быть разделена на оценку вероятности каждой угрозы и оценку последствий воздействия угрозы. Угрозы и риск являются частями итеративного процесса: появление новых угроз возможно при принятии контрмер, например угрозы криптографическим ключам возникают в результате реализации криптографических мер. Понятие намеренной угрозы в информационной безопасности связано с термином атака, под которой понимается несанкционированная деятельность с вредоносным намерением [27].

Классификация и терминология угроз информационной безопасности в разных стандартах ITU-T (например, рекомендации E.408 и X.800) отличаются.

Рассмотрим намеренные угрозы в сетях связи общего пользования, к которым согласно рекомендации ITU-T E.408 [111] могут быть отнесены: нелегальное проникновение, подслушивание, несанкционированный доступ, потеря или искажение информации, непризнание авторства, подлог, отказ в обслуживании.

При угрозе нелегальное проникновение объект предпринимает попытку представить себя другим объектом.

При угрозе подслушивание происходит попытка нарушения конфиденциальности путем наблюдения связью.

При угрозе несанкционированного доступа злоумышленник пытается получить доступ к данным в нарушение действующей стратегии безопасности.

При угрозе потеря или искажение информации целостность переносимых данных поставлена под угрозу из-за несанкционированного уничтожения данных, вставки, изменении содержания, изменении порядка следования, повторной передачи или задержки.

При угрозе непризнания авторства объект, который участвовал в обмене по сети связи, впоследствии отрицает этот факт.

При угрозе подлог объект подделывает информацию и заявляет, что эта информация была получена от другого объекта или передана другому объекту.

При угрозе отказ в обслуживании имеет место невыполнение объектом его функций или препятствование им другим объектам выполнять их функции. Эта угроза может включать

отказ в доступе к сети и отказ в проведении связи.

А.2. Архитектура безопасности сетей связи

Структура сетевой архитектуры безопасности включает принципы описания структуры обеспечения безопасности сети «из конца в конец». Общие положения сетевой архитектуры безопасности изложены в рекомендации международного союза электросвязи ITU-T X.805 [26]. Эта рекомендация закладывает основы для разработки общих и детальных рекомендаций по этим вопросам для конкретных сетей. При изложении материала настоящей работы термин «сетевая безопасность» часто будет заменён широко используемым в литературе равнозначным ему термином «информационная безопасность в сетях» или просто «информационная безопасность» (ИБ).

Архитектура безопасности включает комплексное рассмотрение следующих аспектов ИБ:

- Какие необходимы способы обеспечения ИБ и от каких угроз?
- Какие группы сетевого оборудования должны быть защищены?
- Какие функции сети нуждаются в защите?

Эти вопросы относятся в указанной рекомендации [26] к следующим трём составляющим архитектуры: угрозы ИБ и способы обеспечения безопасности, уровни безопасности и плоскости безопасности. Выше перечислены намеренные угрозы в сетях связи общего пользования согласно рекомендации ITU-T E.408.

А.2.1. Способы обеспечения информационной безопасности

Способы обеспечения информационной безопасности в сетях определяют политику безопасности конкретной сети и включают комплекс мер (характеристик): управление доступом, аутентификация, неотказуемость авторства, конфиденциальность данных, безопасность связи, целостность данных, готовность, приватность. Все эти способы защищают от всех основных угроз ИБ. Согласно рекомендации X.800 под угрозой понимается потенциальное нарушение ИБ.

Управление доступом

Управлением доступом защищает от несанкционированного использования сетевых ресурсов персоналом или устройствами.

Аутентификация

Аутентификация гарантирует подлинность участвующих в связи заявляемой личности,

устройства, услуги или приложения. Это понятие также известно под названием «подлинность источника данных» (data origin authentication).

Неотказуемость

Неотказуемость обеспечивает средства для предотвращения со стороны индивидуума или объекта отрицания выполнения конкретных действий, связанных с сетью (таких как доказательство обязательства, намерения готовности; доказательства источника данных, доказательства использования ресурса). Гарантируется наличие данных, которые могут быть представлены третьей стороне и которые могут использоваться как доказательство того, что некоторое событие имело место.

Конфиденциальность данных

Конфиденциальность данных защищает данные от неправомочного раскрытия. Конфиденциальность данных гарантирует, что содержание данных не может быть понято объектами, которые не имеют на это права.

Безопасность связи

Гарантия того, что информационные потоки проходят между санкционированными пунктами (т.е. информация не изменяет направление и не перехватывается).

Целостность данных

Уверенность в том, что данные не были изменены на пути от отправителя к получателю. Под аутентификацией сообщений понимается одновременное обеспечение подлинности источника сообщения (т.е. его аутентификация) и целостность данных поступившего от него сообщения.

Готовность (доступность)

Гарантия того, что нет отказа санкционированному доступу к устройству сети, хранимой информации, информационным потокам, услугам сети и приложениям. Решения по восстановлению таких отказов включены в эту категории.

Приватность

Гарантия защиты приватной информации пользователя от раскрытия при передаче её по сети. Примером может быть географическое местоположение пользователя мобильной сетью.

А.2.2. Уровни безопасности

Приведённые выше способы обеспечения ИБ применяются к группе оборудования и их функциям с учётом иерархического принципа их деления по уровням. В Рекомендации ITU-T X.805 [26] определено 3 уровня безопасности: уровень безопасности инфраструктуры (Infrastructure Security), уровень безопасности услуг (Services Security) и уровень безопасности приложений (Applications Security).

Уровень безопасности инфраструктуры обеспечивает уровень безопасности услуг, а уровень безопасности услуг обеспечивает уровень безопасности приложений. Для каждого из этих уровней свойственны определённые уязвимости от угроз безопасности и способы защиты от них. Все приведённые выше способы обеспечения безопасности могут применяться к разным уровням безопасности, которые не будем путать с уровнями эталонной модели взаимодействия открытых систем.

Уровень безопасности инфраструктуры относится к функциям основных устройств сети. Примерами таких устройств являются коммутаторы, маршрутизаторы, серверы, а также каналы связи между ними. Уровень безопасности услуг относится к функциям услуг, предоставляемых провайдером пользователю. Примером услуг является виртуальная частная сеть VPN (Virtual Private Network).

Уровень безопасности приложений относится к функциям доступных пользователю приложений. Примером приложений являются электронная почта, передача файлов FTP (File Transfer Protocol) и др.

А.2.3. Плоскости безопасности

Плоскостью безопасности (Security Plane) является определённый вид деятельности в сети, защищённый приведёнными выше способами обеспечения ИБ. В Рекомендации ITU-T X.805 определено 3 типа плоскости безопасности.

- Плоскость безопасности управления сетью (Management Security Plane) Плоскость безопасности управления сетью относится к защите функций администрирования, эксплуатации и обслуживания сети OAM&P (Operation Administration Maintenance&Provision). Управление сетью обеспечивает выполнение процедур, связанных с возникновением отказов, пропускной способностью, администрированием, обслуживанием, безопасностью (FCAPS - Fault, Capacity, Administration, Provisioning, Security). Сообщения, выполняющие указанные процедуры, могут передаваться как в той же полосе пропускания, что и

пользовательский трафик (внутриполосная передача), так и по отдельно выделенным каналам (внеполосная передача).

- Плоскость безопасности транспортной сети (Control Security Plane) Плоскость безопасности транспортной сети относится к защите функций и передаваемой по сети информации, например, по установлению и разъединению соединения (сигнальная информация), по маршрутизации сообщений. В сети Интернет маршрутизация внутриполосная, а в телефонной сети общего пользования ТфОП и в IP-телефонии – внеполосная.
- Плоскость безопасности оконечного пользователя (End-User Security Plane). Плоскость безопасности оконечного пользователя относится к безопасности сети доступа и пользования абонентами сетью поставщика услуг. К этой плоскости безопасности относится также защита потоков данных оконечного пользователя. Оконечные пользователи могут использовать сеть либо только для установления соединения, либо для предоставления им дополнительных услуг (как, например, виртуальная частная сеть), либо для доступа к приложениям сети.

При проектировании сетей связи предъявляется требование, чтобы процедуры в плоскостях безопасности были изолированы друг от друга. Например, возникновение проблем безопасности на плоскости оконечного пользователя не должно распространиться через интерфейс на плоскость безопасности управления сетью.

Концепция безопасности плоскостей позволяет дифференцировать и обеспечить независимость проблем обеспечения ИБ. Например, IP-телефония относится к уровню безопасности услуг. Безопасность плоскости управления сетью, относящаяся к IP-телефонии, должна быть независима от безопасности плоскости транспортной сети (например, безопасности протокола сигнализации), а также должна быть независима от безопасности плоскости оконечного пользователя в части передаваемой информации (например, безопасности пользовательских данных).

А.2.4. Угрозы безопасности и способы обеспечения безопасности

В таблице А.1 приведены способы обеспечения ИБ, соответствующие защите от угроз ИБ из перечня угроз в рекомендации ITU-T X.800. Буква «Y» в таблице означает, что угрозе ИБ, соответствующей столбцу таблицы, противодействует способ обеспечения ИБ, соответствующей строке таблицы.

Таблица А.1. Способы обеспечения ИБ, противодействующие угрозам ИБ

Угрозы безопасности / Способы обеспечения ИБ	Разрушение информации или других ресурсов	Искажения или модификация информации или других ресурсов	Кража, уничтожение или потеря информации или других ресурсов	Раскрытие информации	Прерывание обслуживания
Управление доступом	Y	Y	Y	Y	
Аутентификация			Y	Y	
Неотказуемость	Y	Y	Y	Y	Y
Конфиденциальность данных			Y	Y	
Безопасность связи			Y	Y	
Целостность данных	Y	Y			
Готовность (доступность)	Y				Y
Приватность				Y	

А.2.5. Способы обеспечения ИБ в модулях безопасности

Сочетание каждого уровня безопасности с каждой плоскостью безопасности представляет область (модуль) безопасности, в которой способы обеспечения ИБ применяются для противодействия угрозам. В таблице А.2 приведены составы всех девяти модулей архитектуры сетевой безопасности.

Таблица А.2. Состав модулей архитектуры сетевой безопасности

Уровень безопасности / Плоскость безопасности	Инфраструктуры	Услуги	Приложений

Управления сетью	Модуль 1	Модуль 4	Модуль 7
Транспортной сети	Модуль 2	Модуль 5	Модуль 8
Оконечного пользователя	Модуль 3	Модуль 6	Модуль 9

Поясним таблицу на примерах, приведенных в рекомендации ITU-T E.408 [111]. Под модулем 1 понимается архитектура сетевой безопасности, включающая плоскость безопасности управления сетью и уровень безопасности инфраструктуры. Под модулем 5 понимается архитектура, включающая плоскость безопасности транспортной сети и уровень безопасности услуги. Под модулем 9 понимается архитектура, включающая плоскость безопасности оконечного пользователя и уровень безопасности приложений. Ниже приведём в качестве примера (для модулей 1, 5 и 9) описание способов обеспечения ИБ, соответствующих этим модулям. В таблице А.3 приведён пример, иллюстрирующий применение способов обеспечения ИБ в случае архитектуры сетевой безопасности, соответствующей модулю 1.

Таблица А.3. Способы обеспечения ИБ модуля 1 архитектуры сетевой безопасности (пример)

Способы обеспечения безопасности	Задачи безопасности
Управление доступом	Гарантия того, что только санкционированному персоналу и устройствам сети (например, устройствам, управляемым в IP-сети протоколом SNMP) позволены административные и эксплутационные функции на устройствах сети или линиях связи.
Аутентификация	Проверка идентификатора, личности или устройства, исполняющего административные и эксплутационные функции с устройствами сети и линиями связи.
Неотказуемость авторства	Зарегистрировать индивидуума или устройство, которые принимали участие в административных и эксплуатационных операциях. Эта запись может быть использована для доказательства источника этих действий.
Конфиденциальность данных	Защита аутентификационных данных администратора от несанкционированного доступа или перехвата (например, административные идентификаторы и пароли).

Безопасность связи	В случае удалённого управления сетевыми устройствами и линиями связи гарантируется, что управляющей информацией является только та, которая передаётся между ними (т.е. эта информация доставляется правильному адресату).
Целостность данных	Защита содержания информации сетевых устройств и линий связи от несанкционированной модификации, уничтожения, искажения и повтора.
Готовность (доступность)	Гарантируется готовность управлять сетевыми устройствами или линиями связи санкционированным персоналом, а также то, что устройства не находятся в состоянии отказа. При этом предусматривается защита от отказов в обслуживании DoS (Denial of Service), а также от уничтожения или модификации административной информации аутентификации (например, административные идентификатор и пароли)
Приватность	Гарантируется, что информация, которая может быть использована для идентификации устройств сети и линий связи отсутствует у несанкционированного персонала или в устройствах. Примером такой информации может быть, например, IP-адрес сетевого устройства.

В таблице А.4 приведён пример, иллюстрирующий применение способов обеспечения ИБ в случае архитектуры сетевой безопасности, соответствующей модулю 5 (плоскость безопасности транспортной сети, уровень безопасности услуг).

Таблица А.4. Способы обеспечения ИБ модуля архитектуры сетевой безопасности

Способы обеспечения безопасности	Задачи безопасности
Управление доступом	Гарантия того, что информация управления, полученная устройством сети для сетевой услуги, исходит от санкционированного источника.
Аутентификация	Проверка идентификатора источника информации управления сетевой услугой, отправленного в устройстве сети, участвующего в сетевой услуге.

Неотказуемость авторства	Зарегистрировать индивидуума и устройство, от которых было отправлено сообщения управления сетевой услугой и принято сетевым устройством по обработке сетевой услуги. Зарегистрировать операции, которые при этом были исполнены. Эта запись может быть использована для доказательства источника этих действий.
Конфиденциальность данных	Защита информации управления сетевой услугой, которая находится в устройстве сети (например, базы данных протокола IPSec Интернета), передаётся по сети или содержится изолированно от несанкционированного доступа и анализа содержания. При этом может быть использована техника контроля доступа.
Безопасность связи	Гарантия того, что информация управления сетевой услугой передаётся по сети (например, сообщения согласования ключей протокола IPSec Интернета) только между источником этого сообщения и правильным пунктом назначения.
Целостность данных	Защита информации управления сетевой услугой (находящейся в устройстве сети, во время передачи её по сети или содержащейся автономно) от несанкционированной модификации, уничтожения, искажения и повтора.
Готовность (доступность)	Гарантия того, что устройство сети, которое выполняет функцию сетевой услуги, готово всегда получить информацию управления от санкционированных источников. Эта гарантия включает защиту от отказов в обслуживании DoS.
Приватность	Гарантия того, что информация, которая может быть использована для идентификации устройств сети и линии связи и выполняет функцию сетевой услуги, не имеется у несанкционированного персонала или в несанкционированных устройствах. Примером такой информации может быть, например, IP-адрес сетевого устройства.

В таблице А.5 приведён пример, иллюстрирующий применение способов обеспечения ИБ в случае архитектуры сетевой безопасности, соответствующей модулю 9 (плоскость безопасности оконечного пользователя, уровень безопасности приложений).

Таблица А.5. Способы обеспечения ИБ модуля 9 архитектуры сетевой безопасности

Способы обеспечения безопасности	Задачи безопасности
Управление доступом	Гарантия того, что только санкционированным пользователям и устройствам позволен допуск и использование сетевых приложений.
Аутентификация	Проверка идентификатора пользователя или устройства, пытающихся получить допуск и использовать сетевые приложения. Техника аутентификации может быть затребована, как часть контроля доступа.
Неотказуемость авторства	Зарегистрировать пользователя или устройство при попытке их получить доступ и использовать сетевые приложения. Эта запись может быть использована для доказательства доступа и использования приложения оконечным пользователем или устройством.
Конфиденциальность данных	Защита данных оконечного пользователя (например, номера кредитной карты пользователя), которые транспортируются, обрабатываются и сохраняются сетевым приложением от несанкционированного доступа или обзора. Эти же положения относятся к данным оконечного пользователя, когда они поступают от пользователя к сетевому приложению. Техника, используемая при контроле доступа, может также способствовать обеспечению данных оконечного пользователя.
Безопасность связи	Гарантия того, что данные оконечного пользователя, которые транспортируются, обрабатываются, хранятся сетевым приложением, не отводятся и не перехватываются без санкционированного доступа. Эти же положения относятся к данным оконечного пункта, когда они поступают от пользователя к сетевому приложению.

Целостность данных	Защита данных оконечного пользователя (которые транспортируются, обрабатываются, хранятся в сетевом приложении) от несанкционированной модификации, уничтожения, искажения и повтора.
Готовность (доступность)	Гарантия того, что сетевому приложению, санкционированному оконечному пользователю или устройству не может быть дан отказ в доступе. Предусматривается защита от отказов в обслуживании DoS, а также от уничтожения или модификации аутентификационной информации (например, идентификаторы пользователей и пароли).
Приватность	Гарантия того, что сетевые приложения не предоставляют несанкционированным личностям и устройствам информацию, принадлежащую для использования оконечным пользователем.

А.3. Метод количественной оценки угрозы безопасности сети связи

Согласно Рекомендации МСЭ-Т Е.408 [111] по требованиям к безопасности сетей электросвязи характеристика риска ИБ определяется двумя показателями – вероятностью угрозы безопасности и последствием ее воздействия при атаке злоумышленника (реализации этой угрозы).

Приведем метод количественной оценки угрозы информационной безопасности сети связи, изложенный в документе ETSI ETR 332 [112]. В некоторых документах количественную оценку угрозы информационной безопасности называют риском. В этом методе предлагается общая методология для всех систем сетей связи и заключается в следующем:

- проводится оценка вероятности реализации угрозы P;
- определяется оценка последствий реализации угрозы G;
- рассчитывается произведение P*G;
- составляется ранжированный по этим произведениям список количественных оценок угроз. Согласно документу ETSI ETR 332 может быть использовано четыре оценки угрозы — высокая, средняя, низкая или незначительная.

Все приведенные выше параметры определяются экспертным способом и требуют высокой квалификации и опыта экспертов.

По данным в работе [113] по оценке аналитиков суммарные финансовые потери из-за угроз ИБ составляют от 1% до 5% валового дохода оператора связи. При этом отмечается, что операторы связи стараются не предоставлять сведений о масштабах потерь. При больших доходах они допускают небольшой процент потерь, считая их такими же неизбежными издержками бизнеса, как налоги.

ПРИЛОЖЕНИЕ Б. Шифрование с общим ключом

Одним из основных механизмов обеспечения конфиденциальности данных является шифрование открытого текста. Наука о шифровании/дешифровании называется криптографией (cryptography). Результат шифрования сообщения P, который обозначим через C, образуется с помощью функции Ek, параметром которой является ключ K (т.е. C = Ek(P)). Особенность такой записи состоит в том, что параметр K записан не в виде аргумента функции E, а в виде нижнего индекса. Модель процесса шифрования/дешифрования показана на рис. Б.1.

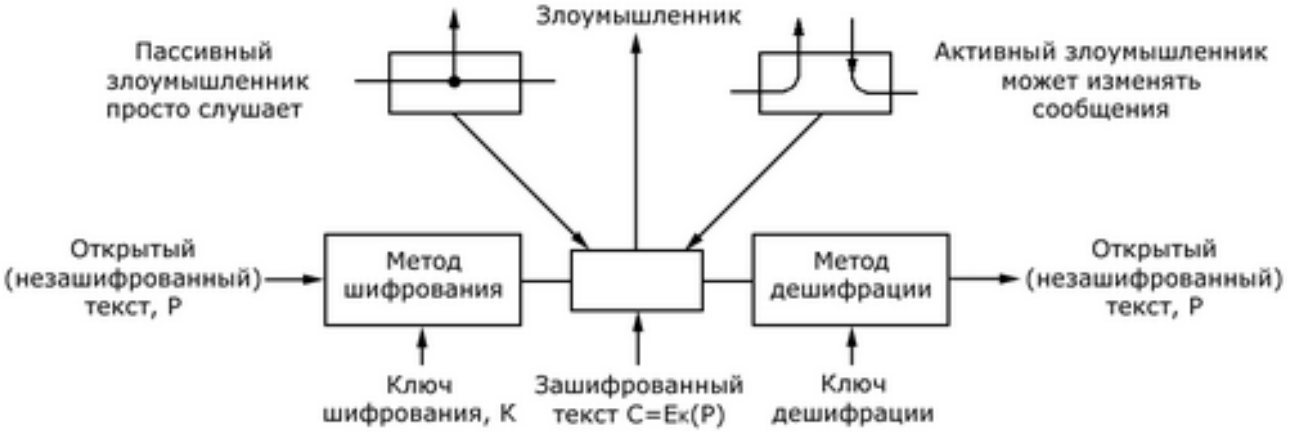


Рис. Б.1. Модель процесса шифрования/дешифрования

Предполагается, что противник или злоумышленник слышит и аккуратно копирует весь зашифрованный текст. Однако в отличие от получателя, которому предназначается данное сообщение, злоумышленник не знает ключа дешифрации, и поэтому расшифровка сообщения представляет для него большие трудности, или она просто невозможна. Иногда злоумышленник может не только прослушивать канал связи (пассивный злоумышленник), но способен также записывать сообщения и воспроизводить их позднее, вставлять свои сообщения или модифицировать исходное сообщение. Искусство взлома шифров называется криптоанализом.

Б.1. Классификация методов шифрования

На рис. Б.2. приведена классификация методов шифрования сообщений. Различают 2 типа алгоритмов шифрования/дешифрования: симметричное (его называют также традиционное или шифрование с общим ключом) и ассиметричное (его называют также шифрование с открытым ключом). Соответственно и криптография называется

симметричной и асимметричной.

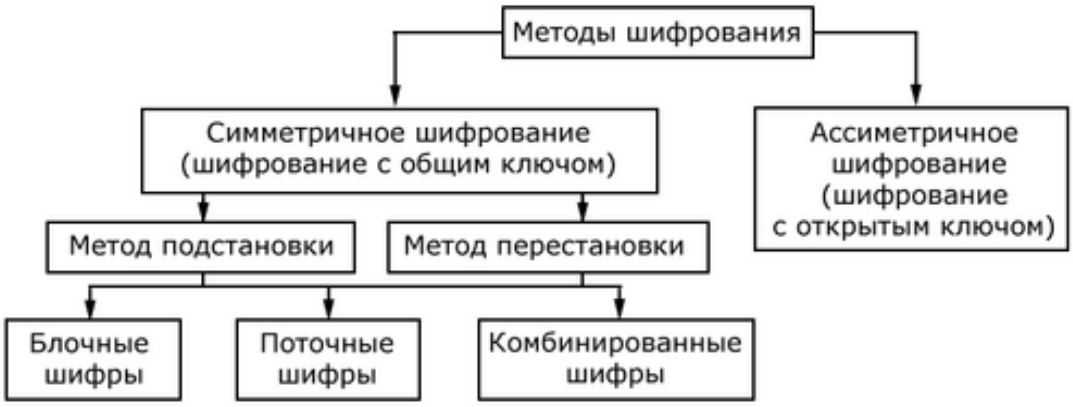


Рис. Б.2. Классификация методов шифрования сообщений

К основному принципу криптографии относится ограничение времени использования одного и того же ключа до минимума путём его частой смены. В криптографии принять считать, что противник может знать используемый алгоритм шифрования, перехваченный шифротекст, но не знает секретный ключ. Это называется правилом «Кирхгоффа».

Настоящая глава посвящена симметричному шифрованию, при котором ключ дешифрования совпадает с ключом шифрования. При дешифрации открытый текст P определяется с помощью функции дешифрования D_k, т.е. $P = D_k(C)$. Подставив зашифрованное значение C в эту формулу, получаем, что $P = D_k(E_k(P))$. Основное правило криптографии состоит в предположении, что криптоаналитику (взломщику кода) известен используемый алгоритм шифрования. Другими словами, злоумышленник точно знает, как работает алгоритм шифрования E_k.

Из-за усилий, необходимых для разработки, тестирования и установки нового метода, каждый раз, когда старый алгоритм оказывался известным или считался скомпрометированным, хранить секрет шифрования просто непрактично. А предположение, что алгоритм остаётся секретным, когда это уже не так, могло бы причинить больший вред. Здесь на помощь приходит ключ шифрования. Ключ состоит из относительно короткой строки, определяющей один из огромного количества вариантов результата шифрования. В отличие от самого метода шифрования, который может изменяться только раз в несколько лет, ключ можно менять так часто, как это нужно.

Секретности алгоритма не стоит придавать большого значения. Попытка сохранить алгоритм

в тайне обречена на провал. К тому же, опубликовав свой алгоритм, разработчик получает бесплатную консультацию от большого количества учёных-криптоаналитиков, горящих желанием взломать новую систему и тем самым продемонстрировать свои ум и учёность. Если никто не смог взломать алгоритм за 5 лет с момента его опубликования, то, по-видимому, этот алгоритм достаточно прочен. Поскольку реально в тайне хранится только ключ, основной вопрос заключается в его длине. Рассмотрим простой кодовый замок. Его основной принцип состоит в том, что вы последовательно вводите десятичные цифры. Все это знают, но ключ хранится в секрете. Ключ длиной в две цифры образует 100 вариантов. Ключ длиной в три цифры означает 1000 вариантов, а при длине ключа в шесть цифр число комбинаций достигает миллиона. Чем длиннее ключ, тем выше показатель трудозатрат взломщика кода. При увеличении длины ключа показатель трудозатрат для взлома системы путём простого перебора значений ключа растёт экспоненциально. Секретность передаваемого сообщения обеспечивается мощным (но всё же открытым) алгоритмом и длинным ключом. Чтобы не дать прочитать свою электронную почту, может быть достаточно 64-разрядного ключа. В коммерческих системах имеет смысл использовать 128-битный код.

С точки зрения криптоаналитика задача криптоанализа имеет 3 варианта. Во-первых, у криптоаналитика может быть некоторое количество зашифрованного текста без соответствующего открытого текста. Во-вторых, у криптоаналитика может оказаться некоторое количество зашифрованного текста и соответствующего ему открытого текста. В этом случае мы имеем дело с проблемой известного открытого текста. Наконец, когда у криптоаналитика есть возможность зашифровать любой кусок открытого текста по своему выбору, мы получаем третий вариант проблемы дешифрации, то есть проблему произвольного открытого текста. Если бы криптоаналитикам было позволено задавать вопросы типа: «Как будет выглядеть зашифрованное ABCDEFGHJKL?», задачи криптоаналитика решались бы легко. Новички в деле криптографии часто полагают, что шифр является достаточно надёжным, если он может выдержать атаку первого типа (только зашифрованный текст). Такое предположение весьма наивно. Во многих случаях криптоаналитик может угадать часть зашифрованного текста. Например, первое, что криптоаналитик получит несколько соответствующих друг другу пар кусков зашифрованного и открытого текста, его работа становится значительно легче. Для обеспечения секретности нужна предусмотрительность криптографа, который должен гарантировать, что система не будет взломана, даже если его оппонент сможет закодировать несколько участков открытого текста по выбору.

Б.2. Блочные шифры

Б.2.1. Методы перестановки и подстановки. Схема блочного шифрования

Настоящий раздел посвящён описанию принципа работы блочных шифров. Существуют 2 метода симметричного шифрования: метод перестановки и метод подстановки. Шифры, основанные на методе **перестановки**, сохраняют порядок символов, но подменяют их. Шифры, использующие метод перестановки, меняют порядок следования символов, но не изменяют сами символы. Ниже приведён простой перестановочный шифр с колоночной перестановкой. Ключом к шифру служит слово или фраза, не содержащая повторяющихся букв. В данном примере в качестве ключа используется слово "М Г Т У Д И П Л". Цель ключа - пронумеровать колонки. Первой колонкой становится колонка под буквой расположенной ближе всего к началу алфавита, и.т.д. Открытый текст записывается горизонтально в строках. Шифрованный текст читается по колонкам, начиная с колонки с младшей ключевой буквы.

М	**Г**	**Т**	**У**	**Д**	**И**	**П**	**Л**
5	1	7	8	2	3	6	4
с	т	у	д	е	н	т	ы
у	ч	а	т	с	я	н	а
х	о	р	о	ш	о	и	о
т	л	и	ч	н	о	4	5

```
Открытый текст: "студентыучатсянахорошоиотлично45".

Зашифрованный текст: "тчолесшнняооыао5сухттни4уаидточ".
```

В шифрах, основанных на методе **подстановки**, каждый символ или группа символов заменяется другим символом или группой символов. Примером этого метода может быть замена одних букв алфавита на другие. Устанавливается соответствие каждого символа открытого текста другому символу в закрытом тексте. Приведём пример, в котором сообщение открытого текста записывается строчными буквами, а зашифрованного текста – прописными.

```
Открытый текст: "a b c d e f g h i j k l m n o p q r s t u v w x w z".

Зашифрованный текст: "Q W E R T Y U I O P A S D F G H J K L Z X C V B N M".
```

Такая система называется моноалфавитной подстановкой, ключом к которой является 26-символьная строка, соответствующая полному алфавиту. В нашем примере слово «attack» будет выглядеть, как «QZZQEA». При симметричном блочном шифровании сообщения разбиваются на отдельные блоки, каждый из которых подлежит отдельно шифрованию/дешифрованию. Большинство алгоритмы блочного шифрования имеют

структуру, впервые описанную Хорстом Файстелем в 1973 году. Соответствующая схема показана на рис. Б.3 [9].

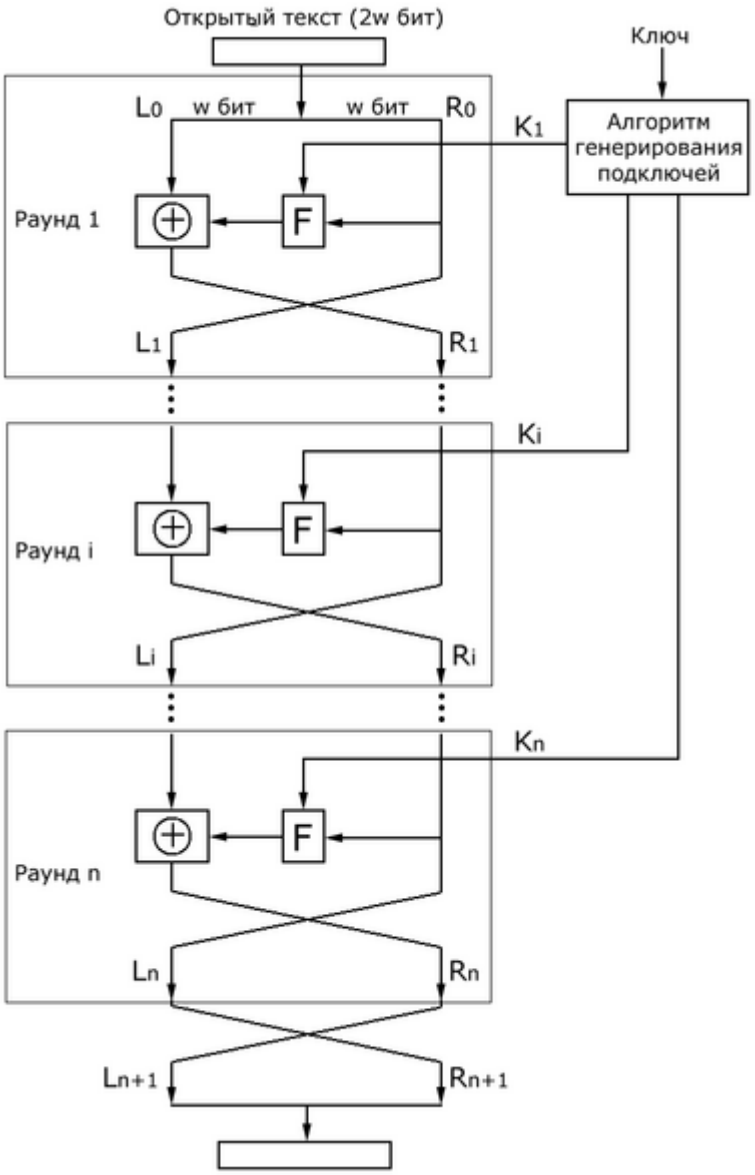


Рис. Б.3. Классическая схема Файстеля

На вход алгоритма шифрования подаётся блок открытого текста длиной 2w бит и ключ K. Блок открытого текста разделяется на 2 равные части L0 и R0, которые последовательно проходят n раундов обработки, а затем объединяются снова для получения блока шифрованного текста соответствующей длины. Для раунда I в качестве входных данных выступают Li-1 и Ri-1, полученные на выходе предыдущего раунда, и подключ Ki, вычисляемый по общему ключу K. В общем случае все подключи Ki отличаются, как от общего ключа, так и друг от друга.

Все раунды обработки проходят по одной и той же схеме. Сначала для первой половины блока данных выполняется операция подстановки. Она заключается в применении к правой половине блока данных некоторой функции раунда F и последующем сложении полученного результата с левой половиной блока данных с помощью операции сложения по модулю два (XOR, исключающее «ИЛИ»). Для всех раундов функция раунда имеет одну и ту же структуру, но зависит от параметра – подключа раунда Ki. После подстановки выполняется перестановка, представляющая собой обмен местами двух половин блока данных.

Практическая реализация схемы Файстеля зависит от конструктивных особенностей и выбора значений для следующих параметров.

- Размер блока. Чем больше размер блока, тем выше надёжность шифра (при прочих равных условиях), но ниже скорость выполнения операций шифрования и дешифрования. Современные блочные шифры длиной блока 64, 128 бит.
- Длина ключа. Чем длиннее ключ, тем выше надёжность шифра, но с увеличением длины ключа скорость шифрования и дешифрования замедляется.
- Число раундов обработки. Суть идеи шифра Файстеля в том, что за один раунд обработки данных обеспечивается недостаточно высокая надёжность шифрования, но стойкость шифра повышается с каждым новым раундом. Число раундов в нескольких американских стандартах шифрования равно 16, в отечественном – 32.
- Алгоритм вычисления подключей. Чем сложнее этот алгоритм, тем труднее криптоанализ шифра.

Процесс дешифрования Файстеля принципиально не отличается от процесса шифрования. Применяется тот же алгоритм, но на вход подаётся шифрованный текст, а подключи Ki используются в обратной последовательности: для первого раунда берётся подключ Kn, для второго – Kn-1 и так далее, пока не будет введён ключ K1 для последнего раунда. Такое свойство этой схемы шифрования оказывается очень удобным, так как для дешифрования не требуется вводить второй алгоритм, отличный от используемого алгоритма шифрования.

Приведём некоторые данные блочных шифров, используемых в сетях. Стандарт шифрования данных DES (Data Encryption Standard) предусматривает работу с блоками данных длиной 64 бита и использует ключ длиной 56 бит. Стандарт шифрования «тройной» DEA (TDEA) использует 3 ключа и трижды применяется алгоритм DES. TDEA использует ключи длиной 112 бита и 168 бит. Открытый текст блока P шифруется в блок C

следующим образом (рис. Б.4.а):

$$C = E_{K_3}[D_{K_2}[E_{K_1}[P]] ,$$

где:

$E_{K_i}[X]$ - шифрование X с использованием ключа K_i;

$E_{K_i}[Y]$ - шифрование Y с использованием ключа K_i.

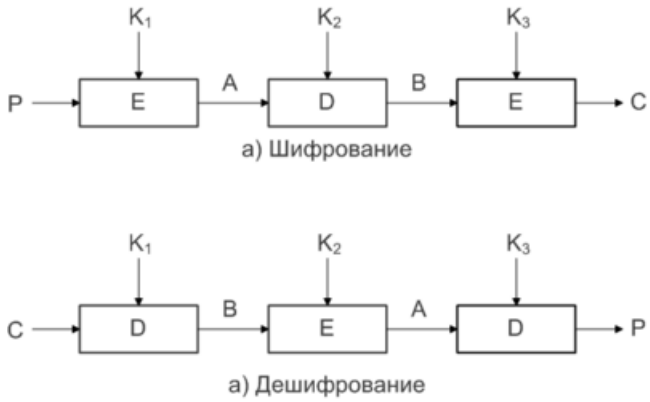


Рис. Б.4. «Тройной» DEA

Дешифрация представляет ту же операцию, выполняемую с ключами в обратном порядке (рис. Б.4. б). То, что на второй стадии используется операция дешифрации, не существенно с точки зрения шифрования, но это даёт возможность пользователям TDEA расшифровать данные, зашифрованные более старой, обычной версией DES, используя один ключ K1:

$$C = E_{K_1}[D_{K_1}[E_{K_1}[P]] = E_{K_1}[P]$$

Международный алгоритм шифрования данных IDEA (International Data Encryption Algorithm) явился одной из первых альтернатив DES и использует 128-битные ключи. Улучшенный стандарт шифрования AES (Advanced Encryption Standard) был принят в 2001 году в результате открытого международного конкурса. AES предусматривает размер блока 128 бит и длину ключа 128, 192 или 256 бит. Использование алгоритма DES допускается

только в действующих системах. Одновременно существование TDEA и AES позволяет осуществить плавный переход к AES. Российский блочный шифр ГОСТ 28147-89, как следует из обозначения его, был принят в качестве стандарта в 1989 году [114]. Основные параметры этого стандарта: длина ключа 256 бит, размер блока 64 бита, 32 раунда. В отличие от DES, ГОСТ 28147-89, до недавнего времени не был предметом столь глубокого анализа со стороны мирового криптографического сообщества. Тем не менее, как отмечают специалисты, величина основных параметров (длина ключа, размер блока, количество раундов) позволяют утверждать, что шифр вряд ли может быть слабым. Никаких эффективных атак против шифра 28147-89 не опубликовано.

Б.2.2. Режимы блочного шифрования

Симметричный блочный шифр обрабатывает блоки данных по одному. В DES, TDEA и ГОСТ 28147-89 длина блока равна 64 бита, в AES – 128 бит. Для более длинных фрагментов открытый текст необходимо разбить на блоки (дополнив последний блок битами заполнителя, если это необходимо). Дальнейшая обработка блоков называется режимом блочного шифрования. Рассмотрим некоторые из наиболее часто используемых режимов.

Б.2.2.1. Режим электронного шифроблокнота (ECB)

На рис. Б.5. показана схема простейшего режима – режима электронного шифроблокнота ECB (Electronic Code Book). В режиме ECB производится независимое шифрование каждого блока на одном и том же ключе K_{AB}.

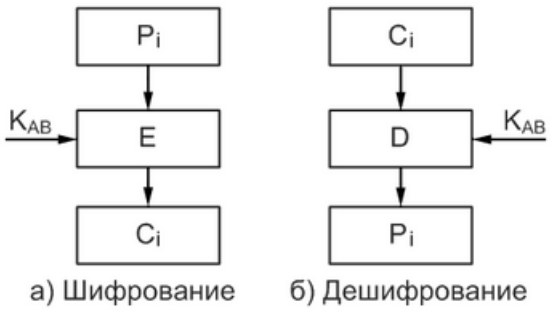


Рис. Б.5. Режим электронного шифроблокнота (ECB)

Если в режиме ECB в сообщении присутствуют одинаковые 64-битовые блоки открытого текста, в шифрованном тексте они тоже будут представляться одинаковыми блоками. Поэтому при передаче достаточно длинных сообщений режим ECB может не обеспечивать необходимый уровень защиты. У криптоаналитика появляется возможность использовать регулярности текста. Например, если известно, что в начале сообщения всегда размещается определённый заголовок, криптоаналитик может получить в своё распоряжение целый набор соответствующих пар блоков открытого и шифрованного текста. Если же сообщение содержит повторяющиеся элементы с периодом повторения, кратным 64 бит, такие элементы тоже могут быть выявлены аналитиком. Подобные сведения упрощают задачу криптоанализа и открывают возможность замещения или реорганизации блоков текста передаваемого сообщения. Данный режим нечувствителен также к выпадению, вставке целого числа блоков, замене блоков.

Все остальные режимы реализуют схемы шифрования свободные от недостатков режима ECB. При этом производится сцепление зашифрованных блоков. В случае повторения в сообщении уже встретившегося ранее блока открытого текста эти режимы позволяют генерировать блок шифрованного текста, отличный от сгенерированного ранее. Приведём два из таких режимов, называемый режимом группового шифра OFB и режим счётчика CTR.

Б.2.2.2. Режим группового шифра (OFB)

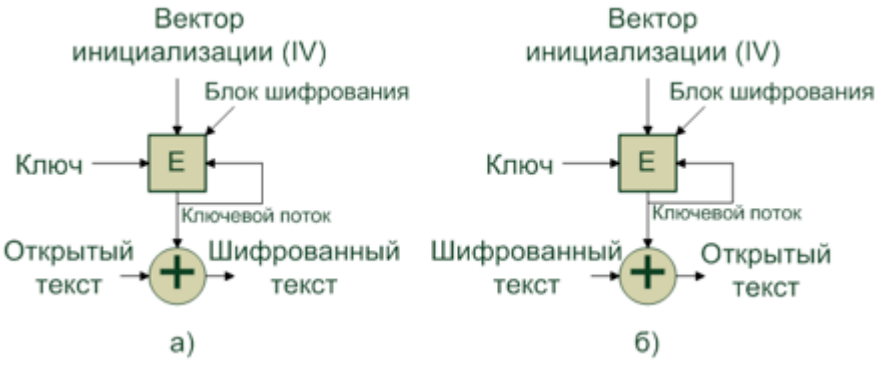


Рис. Б.6. Режим группового шифра (OFB): шифрование (а); дешифрование (б)

На рис. Б.6. приведена схема группового шифра OFB (Output Feedback). Первый раз выходной блок создаётся с помощью ключа блочным шифрованием случайного значения вектора инициализации IV (Initialization Vector). Затем этот выходной блок снова шифруется,

в результате получается второй выходной блок. Для получения третьего блока шифруется второй блок и т.д. Последовательность (произвольной длины) выходных блоков, называемая ключевым потоком, воспринимается как одноразовый блокнот и по модулю 2 складывается с открытым текстом. В результате получается шифрованный текст, как показано на рис. Б.6, а. Обратите внимание: вектор инициализации используется только на первом шаге. После этого шифруются выходные блоки. Кроме того, ключевой поток не зависит от данных, поэтому он в случае необходимости может быть вычислен заранее (что повышает скорость шифрования). Пример дешифрования показан на рис. Б.6, б.

Дешифрование осуществляется путём генерации точно такого же ключевого потока на принимающей стороне. При таком режиме сцепления одинаковым блокам открытого текста не соответствуют одинаковые блоки зашифрованного текста. Замена одного блока вызывает повреждение других блоков открытого текста после их расшифровки.

Б.2.2.3. Режим счётчика (CTR)

Название данного режима происходит от слова «counter» - «счётчик». Всем режимам, кроме электронного шифроблокнота ECB присущ недостаток: доступ к произвольной части зашифрованных данных невозможен. Например, если файл передаётся по сети и затем хранится на диске в зашифрованном виде.

Однако доступ к дискам зачастую бывает необходимо осуществлять в произвольном порядке. Особенно это касается файлов баз данных. Если файл зашифрован в режиме сцепления блоков, придётся вначале дешифровать все блоки, предшествующие нужному. Такой способ работы неудобен. По этой причине был введён ещё один режим шифрования – режим счётчика. Он показан на рис. Б.7. Здесь открытый текст не шифруется напрямую. Вместо этого шифруется вектор инициализации плюс некоторая константа, а уже получающийся в результате шифр складывается по модулю 2 с открытым текстом. Сдвигаясь на 1 по вектору инициализации при шифрации каждого нового блока, можно легко получить способ дешифрации любого места файла. При этом нет необходимости расшифровывать все предшествующие блоки.

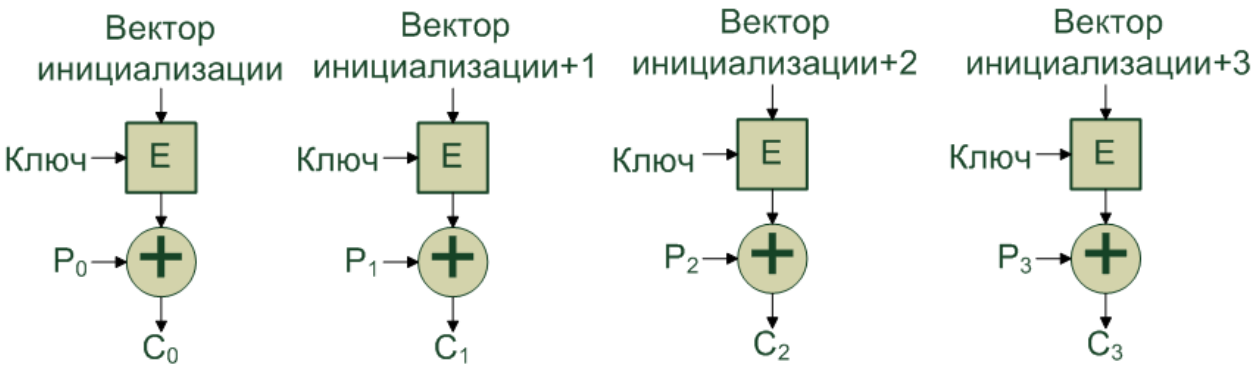


Рис. Б.7. Шифрование в режиме счётчика

Б.3. Поточные шифры

Настоящий раздел посвящён описанию принципа работы поточных шифров.

Простейшей и в то же время самой надёжной схемой симметричного шифрования является так называемая схема однократного использования (рис. Б.8).

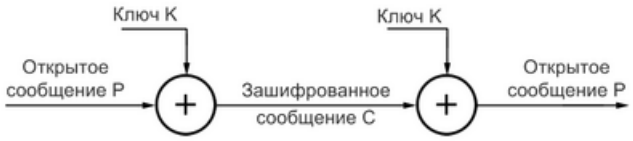


Рис. Б.8. Схема однократного использования поточного шифра

Формируется m-разрядная случайная двойная последовательность – ключ шифра, известный отправителю и получателю сообщения. Отправитель производит побитовое сложение по модулю 2 (операция XOR, «исключающее ИЛИ») ключа и m-разрядной двоичной последовательности, соответствующей открытому сообщению P.

$$C_i = K_i \oplus P_i, i = 1..m,$$

где P_i, K_i и C_i – очередной i-бит соответственно исходного сообщения, ключа и зашифрованного сообщения, m – число битов открытого сообщения P.

Процесс расшифровки сводится к повторной генерации ключевой последовательности и наложению её на зашифрованные данные. Уравнение расшифровки имеет вид:

$$P_i = K_i \oplus C_i = K_i \oplus K_i \oplus P_i$$

К. Шенноном доказано, что если ключ является истинно случайной двоичной последовательностью, причём его длина равна длине исходного сообщения и используется

этот ключ только один раз, то такой шифр является абсолютно стойким, его невозможно раскрыть. Необходимые и достаточные условия абсолютной стойкости шифра:

- полная случайность ключа;
- равенство длин ключа и открытого сообщения;
- однократное использование ключа.

Выполнение этих требований делает такую схему пригодной для массового использования. На эти условия могут согласиться разве что дипломаты, военные и спецслужбы. Таким образом, возникает задача разработки схемы такого теоретически нестойкого шифра, которая использует ключ небольшой разрядности. Этот ключ выполняет функцию «зародыша», порождающего значительно более длинную ключевую последовательность. Такой «зародыш» является входной последовательностью псевдослучайных чисел ПСП (PRNG - pseudo-random number generation). На рис. Б.9 показан такой метод шифрования сообщений, называемый гамма-наложение по модулю 2 открытого текста P на последовательность блоков гаммы шифра γ, полученную с выхода генератора G псевдослучайных последовательностей ПСП.

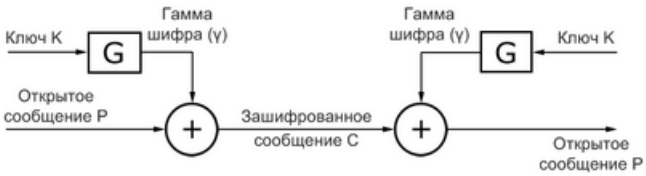


Рис. Б.9. Шифрование сообщения методом гаммирования

Последовательность называется псевдослучайной, если по своим статистическим свойствам она неотличима от истинно случайной, но в отличие от последней является детерминированной, т.е. знание алгоритма её формирования даёт возможность её повторения необходимое число раз.

Надёжность шифрования методом гаммирования определяется качеством генератора гаммы. Приведённая схема шифрования относится к поточным шифрам (stream cipher). В отличие от блочных, поточные шифры осуществляют поэлементное шифрование потока данных без задержки в криптосистеме. Таким образом, обеспечивается шифрование практически в реальном времени. Приведённая на рис. Б.8 схема относится к синхронным поточным

шифрам, при которой отсутствует эффект размножения ошибок, т.е. число искажённых битов в зашифрованной последовательности равно числу искажённых элементов расшифрованной последовательности, пришедшей из канала связи. Нарушение синхронизации приводит к неправильному расшифрованию всех последующих бит. Примером поточного шифрования является алгоритм RC4.

Приведённые выше в разделах Б.2.2.2 и Б.2.2.3 режимы блочного шифрования являются примерами комбинированного шифрования, которое включает блочное и поточное шифрование.

ПРИЛОЖЕНИЕ В. Шифрование с открытым ключом

Основной проблемой использования шифрования с симметричным ключом является проблема распределения ключей. Так как в этом случае шифрование и дешифрование выполняется с помощью одного и того же ключа в сети связи с N абонентами, потребуется число ключей, равное N(N-1)/2. Необходимость наличия недоступных для нарушителя секретных каналов обмена ключами делает практически неприемлемым такой подход для большинства сетей. Эти ключи должны быть сгенерированы и надёжно распределены среди всех участников обмена сообщениями. В настоящем приложении приводится описание шифрования с открытым ключом, одной из функций которого является распределение ключей (управление ключами) симметричного шифрования.

В.1. Принцип шифрования с открытым ключом

Ещё в 40-х годах К.Шеннон предложил строить шифрование таким образом, чтобы задача его вскрытия была эквивалентна решению математической задачи, требующей объёма вычислений недоступного для современных компьютеров. Реализация этой цели стала возможной, когда в 70-х годах Диффи и Хеллман предложили принципиально новый способ без предварительного обмена ключами, так называемое шифрование с открытым ключом. При этом ключ шифрования и ключ дешифрования должны быть различными, причём, знание одного из них не даёт практической возможности определить второй. Предложенные ими алгоритм шифрования E открытого сообщения M и алгоритм его дешифрования D должны удовлетворять следующему требованию: D(E(M))=M, т.е. применив алгоритм дешифрования D к зашифрованному сообщению E(M), мы получаем открытый текст M. Этот метод работает следующим образом.

Некто, например, Алиса (A) желает получить секретное сообщение. Для этого формируются алгоритмы шифрования и дешифрования, удовлетворяющие перечисленному выше требованию. Оба алгоритма и ключ алгоритма шифрования открыто объявляются, отсюда название – шифрование с открытым ключом. Это можно сделать, например, разместив открытый ключ на сайте Алисы. Для обозначения алгоритма шифрования при шифровании открытым ключом A (Алисы) мы будем использовать запись E_A. Для обозначения алгоритма дешифрации персональным секретным личным ключом Алисы мы будем использовать запись D_A.

Аналогично абонент B (Боб) делает то же самое, открыто объявляя E_B, но храня в тайне D_B. Рассмотрим установку надёжного секретного канала между абонентами A и B, которые никогда ранее не встречались. Отметим, что все пользователи сети могут опубликовать свои открытые ключи. Абонент A (отправитель) зашифровывает открытым ключом абонента B (получателя) своё сообщение M, т.е. вычисляет $E_B(M)$ и посылает его абоненту B. Абонент B расшифровывает его с помощью своего секретного личного ключа D_B, т.е. вычисляет $M=D_B(E_B(M))$. Это показано на рис. В.1, а). Кроме абонента B никто не может прочитать это зашифрованное сообщение $C=E_B(M)$ так, как получить ключ D_B на основании известного открытого ключа E_B практически невозможно. На рис. В.1, б) показана передача зашифрованного сообщения M_1 в обратном направлении. $C_1=E_A(M_1)$, т.е. открытым ключом абонента A. Это сообщение абонента B будет расшифровано закрытым личным ключом A, т.е. $M_1=D_A(E_B(M_1))$. Таким образом, A и B получают надёжный секретный канал связи.

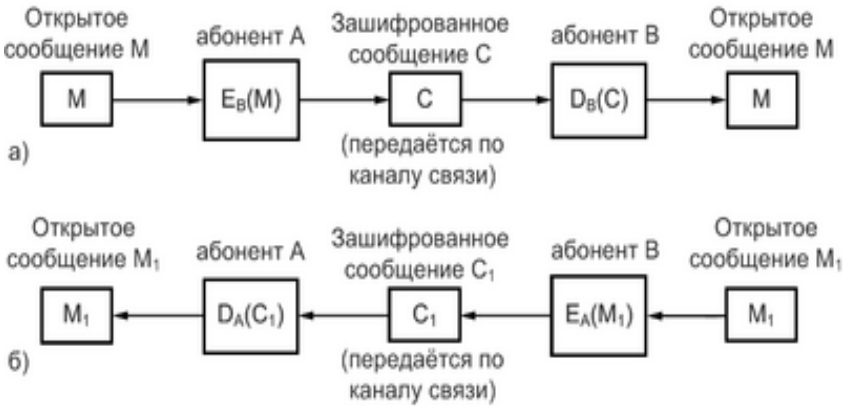


Рис. В.1. Схема шифрования/дешифрования сообщений открытым/закрытым ключом

Обратим внимание на используемую терминологию ключей. Шифрование с открытым ключом предполагает у каждого пользователя наличие двух ключей – открытого ключа, используемого всеми для шифрования сообщений, посылаемых этому пользователю, и закрытого личного ключа, необходимого пользователю для дешифрации приходящих к нему сообщений. Эти ключи мы будем и далее называть открытым и закрытым (личным), чтобы отличить их от секретных ключей, используемых для шифрования и дешифрации в традиционной криптографии с симметричным ключом. Эти ключи мы будем называть общими ключами. Односторонняя функция – это функция, которая легко выполняется в

одном направлении (легко выполняет прямую операцию), но для которой очень трудно выполнить обратную операцию. Примером двухсторонней функции является возведение в степень, ведь легко вычислить 23^8 и также легко вычислить $\sqrt[3]{8}=2$..

Криптосистемы с открытым ключом используют односторонние функции, применяя при этом модульную арифметику. В таблице В.1 приведено сравнение значений для x = 1,2,3,4,5,6 обычной арифметики (вычисление 3^x) и модульной арифметики (вычисление функции 3^x по модулю 7). Значение в таблице $3^x mod 7 = 1$ при значении $x = 6$ означает остаток 1 от деления 3^6 на 7. Обычная запись в модульной арифметике будет выглядеть, как $3^6 = 1 mod 7$.

Таблица В.1. Сравнение обычной арифметики и модульной арифметики

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
3^xmod(7)	3	2	6	4	5	1

Как видно из таблицы В.1, легко вычислить для функции $v^x = y mod(z)$, где $v = 3$, $z = 7$, прямую операцию (т.е. определить остаток y при разных x), так и обратную операцию (т.е. определить x при известном y). Это имеет место для малых значений параметров v,x,y,z. Прямую операцию при больших значениях v и z также легко определить y при разных x (например для функции $y = 543^x mod(21997)$). Однако, обратную операцию (например, вычислить x при заданном y = 5787, т.е. $543^x = 5787 mod 21997$) выполнить невозможно, даже используя сверхбыстрые современные ЭВМ.

Существует много систем шифрования с открытым ключом, наиболее известные из которых – криптосистема RSA и криптосистема Эль-Гамаля. Применение шифрования с открытым ключом позволяет:

- избавиться от необходимости секретных каналов связи для предварительного обмена ключами;
- свести проблему взлома шифра к решению трудной математической задачи, т.е. в конечном счёте принципиально по-другому подойти к обоснованию стойкости криптосистемы;
- решать средствами криптографии задачи, отличные от шифрования (например, задачу обеспечения юридической значимости электронных документов).

B.2. Алгоритм RSA

Один из алгоритмов с открытым ключом был разработан в 1978 году. Он назван по начальным буквам фамилий трёх разработчиков Массачусетского технологического института: RSA (Rivest, Shamir, Adleman). Этот метод к настоящему моменту выдерживает попытки взлома и считается очень прочным. На его основе построены многие практические системы безопасности. Главным недостатком шифрования с открытым ключом является его медленная работа по сравнению с алгоритмами симметричного шифрования. Поэтому шифрование/дешифрование сообщений обычно производится с помощью криптографии с общим ключом, передача этого ключа другому абоненту соединения с помощью асимметричной криптографии.

Для обеспечения достаточной защищённости в RSA требуется ключ длиной, по крайней мере, 1024 бита (против 256 бит в алгоритме AES с симметричными ключами). Опишем в общих чертах, как пользоваться алгоритмом RSA. Создаётся закрытый и открытый ключи абонента. Для этого:

- Выбираем два больших простых числа p и q (обычно длиной 1024 бита). Целое число a>1 называется простым, если его делителями являются только числа ±1 и ±a.
- Определяем значения $n = pq$ и $z = (p - 1)(q - 1)$.
- Выбираем число d, которое является закрытым ключом абонента. Значение d должно быть взаимно простым с числом z.Целые числа d и z являются взаимно простыми, если они не имеют общих простых делителей, т.е. если их единственным общим делителем является 1. Например, числа 8 и 15 являются взаимно простыми, поскольку делителями числа 8 являются 1, 2, 4 и 8, а делителями числа 15-1, 3, 5 и 15, так, что 1 оказывается единственным числом, присутствующим в обоих списках.
- Находим такое число e (которое является открытым ключом абонента), что остаток от деления произведения ed на число z равен 1, т.е. $ed = 1(modz)$ или $e = d^{-1} modz$.

Можно определить ключи d и e в другой последовательности, т.е. сначала e, потом d. Тогда п.3 определяет число e, а п.4 – число d. После вычисления этих параметров можно начинать шифрование. Сначала разбиваем весь открытый текст (рассматриваемый в качестве битовой строки) на блоки так, чтобы каждое сообщение M попало в интервал 0<M<n.

Для того, чтобы зашифровать сообщение M вычисляем $C = M^e(modn)$. Чтобы расшифровать

C и получить открытый текст, вычисляем $M = C^d(modn)$. В этом случае e и d являются соответственно открытым и закрытым ключами получателя. Если абонент А отправляет сообщение М абоненту В, то e и d являются ключами абонента В. В качестве М обычно используют общий ключ симметричного шифрования. Асимметричная криптография позволяет осуществить обмен общими ключами по сети связи общего пользования. Шифрование всего сообщения с помощью алгоритма с открытым ключом имеет недостаток в низкой скорости, т.к. эта операция требует большой производительности процессора. Поэтому для шифрования сообщений используется симметричная криптография (с общим ключом). Поскольку длина общего ключа шифрования небольшая, асимметричная криптография позволяет произвести обмен этими ключами.

Можно показать, что для всех значений М в указанном диапазоне функции шифрования и дешифрации являются взаимно обратными. При этом сообщение М отправляется от абонента В абоненту А (т.е. сообщение шифруется $C_1 = M^d(modn)$ закрытым ключом d и расшифровывается открытым ключом e абонента В). Здесь e и d являются ключами отправителя. В этом случае используются данные для электронного документообмена с помощью электронно-цифровой подписи. Приведём пример шифрования и дешифрования сообщения М соответственно открытым (e) и закрытым (d) ключами получателя В (рис. В.2). Сообщение передаётся отправителем А.

Исходные данные: p=17, q=11, M=88 (p и q – простые числа).

а) Находим n=p•q=17•11=187, 0<M<n, z = (p − 1)(q − 1) = 160

б) Выбираем e=7 (взаимно простое число с z).

в) Определяем закрытый ключ d из выражения $7d = 1 mod 160$ или $d = 7^{-1} mod 160$.

г) Получаем d=23.

Тогда $C = 88^7 mod 187$. Для упрощения таких задач, требующих возведения больших величин в большие степени, используются правила модульной арифметики.

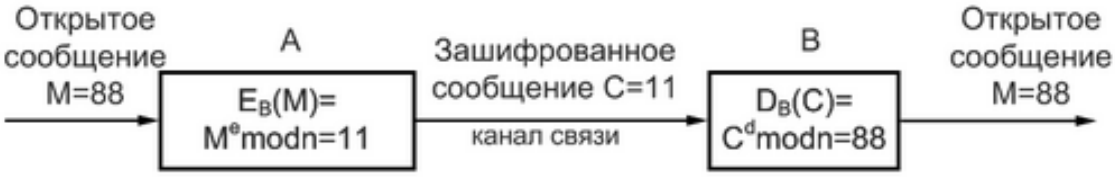
Тогда C = 887mod187 = [(884mod187)(882mod187)(881mod187)]mod187

$88^4 mod 187 = 59969536 mod 187 = 132$

$88^2 mod 187 = 7744 mod 187 = 77$

$88^1 mod 187 = 88$

$M = 11^23 mod 187 = [(11^1 mod 187)\ (11^2 mod 187)\ (11^4 mod 187)\ (11^8 mod 187)\ (11^8 mod 187) = 88$



Оглавление

Рис. В.2. Пример шифрования/дешифрования сообщения открытым/закрытым ключом получателя

Таким образом, открытый ключ состоит из пары (e, n), а закрытый ключ – из пары (d, n). В приведённом примере это соответственно (7, 187) и (23, 187). Надёжность метода обеспечивается сложностью нахождения множителей больших чисел. Если бы криптоаналитик мог разложить на множители открытое число n, он мог бы тогда найти значения p и q, а следовательно, и число z. После этого ключи e и d можно найти при помощи алгоритма Евклида. В настоящем материале этот алгоритм не приводится. Длина блока открытого текста при выборе больших p и q в алгоритме RSA больше, чем в случае симметричного шифрования. Если p и q порядка 2^{512}, тогда n порядка 2^{1024}. В этом случае каждый блок для RSA мог бы содержать до 1024 бит, т.е. больше по сравнению с длинами блоков алгоритма DES (64 бита) или алгоритма AES (128 бит).

В.3. Электронная цифровая подпись (ЭЦП)

Подлинность различных бумажных документов определяется наличием или отсутствием авторизованной рукописной подписи. После появления криптографии с открытым ключом произошла настоящая революция в современных компьютерных и сетевых технологиях. В настоящее время при помощи этих технологий ежедневно проводятся расчёты и совершаются сделки на многие миллиарды долларов, рублей, евро и т.п. Одним из важных элементов этих технологий является электронная цифровая подпись (ЭЦП), которая является реквизитом электронного документа, предназначенным: для защиты данного электронного документа от подделки; идентифицировать владельца сертификата ключа подписи; установить отсутствие искажения информации в электронном документе. Во многих странах и, в частности, в России это понятие введено в гражданское законодательство.

В.3.1. Требования к ЭЦП

Прежде, чем начать рассмотрение криптографической цифровой подписи, сформулируем некоторые свойства, которым (в идеале) должна удовлетворять любая, в частности, обычная рукописная подпись:

- подписать документ может только «законный» владелец подписи (и следовательно, никто не может подделать подпись);
- автор подписи не может от неё отказаться;
- в случае возникновения спора возможно участие третьих лиц (например, суда) для установления подлинности подписи.

Цифровая подпись также должна обладать всеми этими свойствами. 6 апреля 2011 г. был подписан закон «Об электронной цифровой подписи», целью которого «является обеспечение правовых условий использования ЭЦП в электронных документах, при соблюдении которых ЭЦП признаётся равнозначной собственноручной подписи в документе на бумажном носителе» [115].

Проблема замены рукописной подписи требует выполнения трёх способов обеспечения информационной безопасности:

- аутентификация отправителя документа (т.е. получатель сообщения должен быть уверен в том, что данные пришли из указанного в нём источника);
- целостность данных полученного документа (т.е. уверенность в том, что сообщение не было изменено);
- неотказуемость отправителя и получателя для того, чтобы отправитель не мог позднее изменить подписанное сообщение.

Как отмечено в разд. А.2.1 приложения А, одновременная реализация первых двух из указанных способов обеспечения ИБ называется аутентификацией сообщений. Выполнение этих требований важно во многих сферах деятельности и, в частности, в финансовых системах. Когда компьютер клиента заказывает компьютеру банка купить тонну золота, банковский компьютер должен быть уверен, что компьютер, пославший заказ, действительно принадлежит компании, со счёта которой следует снять денежную сумму. Другими словами, банк должен иметь возможность установить подлинность клиента (а клиент – подлинность банка). Также необходима защита банка от мошенничества. Предположим, что банк покупает тонну золота, и сразу после этого цена на золото резко падает. Бесчестный клиент может подать в суд на банк, заявляя, что он никогда не посылал заказа на покупку золота. Банк может показать сообщение в суде, но клиент будет отрицать, что посылал его. Таким образом, должно быть обеспечено требование невозможности отречения от данных ранее обязательств. Необходима и важна также защита клиента в случае, если цена на золото после его покупки банком взлетает вверх и банк пытается создать подписанное сообщение, в котором клиент просит купить не одну тонну золота, а один слиток. Алгоритм создания и проверки достоверности ЭЦП основан на использовании криптографии с открытым ключом с помощью шифрования сообщения закрытым ключом отправителя и дешифрования его открытым ключом. Это обеспечивает все три приведенных выше способа ИБ-аутентификацию отправителя, целостность данных и неотказуемость.

В.3.2. ЭЦП на основе шифрования профиля сообщения

Шифрование всего сообщения с помощью алгоритма с открытым ключом имеет недостаток в низкой скорости, т.к. эта операция требует большой производительности процессора. Это относится к созданию цифровой подписи путём шифрования всего сообщения закрытым ключом отправителя. Для того, чтобы преодолеть эти трудности, используется так называемая односторонняя хеш-функция. Под хеш-функцией понимается функция, отображающая передаваемое сообщение произвольной длины в значение фиксированной длины, называемое хеш-кодом (профилем или дайджестом сообщения). Длина профиля сообщения зависит от используемого алгоритма хеш-функций для его образования. Для широко используемых стандартов хеш-функций MD5 и SHA-1 длина профиля равна соответственной 128 и 160 бит, что обычно существенно короче сообщений.

Создавая цифровую подпись, не всегда требуется соблюдение секретности передаваемого сообщения. Получателю передаётся открытое сообщение вместе с его профилем. Для того, чтобы профиль сообщения выполнял требования к цифровой подписи при его получении от отправителя, он должен обладать следующими свойствами:

- должен быть применимым к блоку данных (сообщению) любой длины;
- длина профиля должна быть фиксированной;
- по заданному открытому тексту сообщения P необходимо легко сосчитать значение профиля этого сообщения. Алгоритм вычисления должен быть практически эффективным и легко вычисленным с точки зрения как аппаратной, так и программной реализации;
- по профилю должно быть практически невозможно определить значение открытого текста P;
- для данного сообщения P практически невозможно подобрать другое сообщения P', чтобы профили этих сообщений совпадали. Это предотвращает возможность фальсификации передаваемого сообщения P;
- изменение хотя бы одного бита входного сообщения должно приводить к совсем другому результату.

Вычисление хеш-кода сообщения не обеспечивает подтверждения подлинности документа и подписи потому, что атакующий может изменить документ и заново вычислить хеш-функцию. Поэтому в целях защиты зашифровывается и сам профиль. Использование короткого (по длине) профиля позволяет шифровать его значительно быстрее, чем шифруется всё сообщение с помощью криптографии с открытым ключом.

Предпоследнее условие предусматривает защиту от действия противника по следующей схеме: сначала перехватывается открытое сообщение вместе с присоединённым к нему шифрованным профилем, затем вычисляется по сообщению профиль и создаётся альтернативное сообщение с тем же профилем. Покажем использование профиля сообщения MD (message digest) при создании цифровой подписи.

Обозначим профиль сообщения P через h(P) и приведём схемы формирования ЭЦП сообщения криптографии с открытым ключом.

На рис. В.3 приведена схема ЭЦП профиля сообщения P с применением криптографии с открытым ключом. Как видно из рисунка, отправитель сообщения P (Алиса) вычисляет профиль сообщения h(P), создаёт ЭЦП с помощью своего закрытого ключа DAh(P) и затем посылает открытое сообщение P с ЭЦП – P, DAh(P) Бобу. Боб с помощью открытого ключа Алисы EA определяет профиль сообщения h(P)=EA(DA(h(P))). Одновременно из полученного сообщения P определяет профиль h'(P). Если оба профиля совпадают, значит все способы информационной безопасности обеспечены цифровой подписью полученного сообщения – аутентификация, целостность данных и неотказуемость.

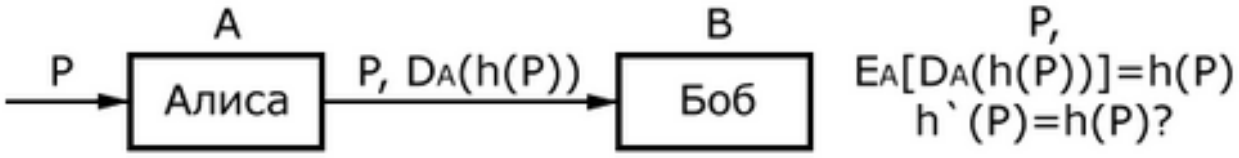


Рис. В.3. ЭЦП на основе профиля сообщения и шифрования с открытым ключом

На основе хеш-функции используется также другой упрощенный способ аутентификации с обеспечением целостности передаваемого сообщения без шифрования и с использованием общего секретного ключа у аутентифицирующей и аутентифицируемой стороны. Передатчик отправляет хеш-функцию обобщенного сообщения вместе с ключом. Профиль этого сообщения гарантирует, что никто не сможет определить ключ во время пересылки, а значит, и не может изменить или создать новое сообщение.

В.3.2.1. Функция хеширования стандарта SHA-1

Все функции хеширования построены на следующих общих принципах.

Вводимое сообщение рассматривается как последовательность l-битовых блоков. Данные,

поступающие на вход схемы хеширования, обрабатываются блок за блоком, в результате чего получается n-битовое значение профиля сообщения (кода хеширования). Приведём краткое описание функции хеширования одного из стандартов. Один из наиболее широко применяемых – безопасный алгоритм хеширования (SHA, Secure Hash Algorithm) был выпущен в 1995 году и получил название SHA-1. Длина профиля сообщения n=160 бит. Длина обрабатываемого блока сообщения L=512 бит. На рис. В.4 представлен общий процесс обработки сообщения с целью получения его профиля.

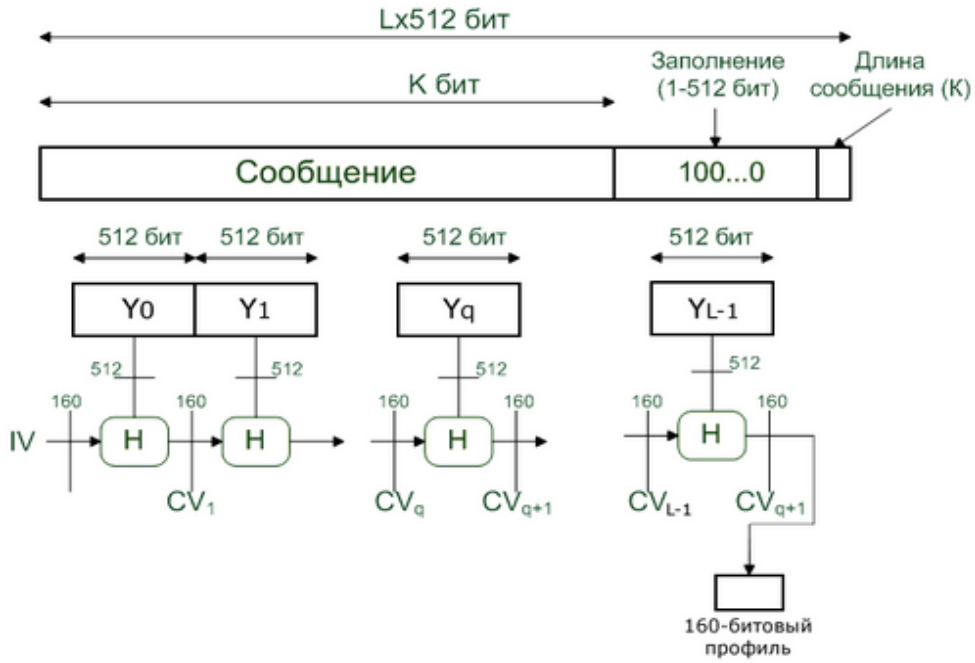


Рис. В.4. Процесс создания профиля сообщения по алгоритму стандарта SHA-1

Обработка состоит из следующих этапов:

- добавление битов заполнителя. Сообщение дополняется так, чтобы длина последнего блока была равна 448 по модулю 512 (длина равна 448 mod 512). То есть длина сообщения на 64 бита меньше, чем число кратное 512. Таким образом, число дополнительных битов находится в диапазоне от 1 до 512. Заполнитель состоит из бита 1, за которым следует необходимое число 0-битов.
- дополнение сообщения. К сообщению добавляется блок из 64 бит. Этот блок рассматривается, как длина сообщения без добавленных битов заполнителя. Включение значения длины затрудняет атаку, которая называется атакой заполнения.

В результате расширения сообщение представляет собой целое число длиной, кратной 512 бит. На рис. В.4 расширенное сообщение представлено последовательностью 512-битовых

блоков $Y_0, Y_1, \ldots Y_{l-1}$ так, что общая длина равна L*512 бит, где L – число блоков.

Для хранения промежуточных и конечных результатов функции хеширования используется 160-битовых буфер, который при обработке первого блока инициализируется с помощью вектора инициализации IV. Основой алгоритма обработки блока длиной 512 бит служит модуль, включающий четыре этапа обработки, каждый из которых состоит из 20 шагов. Все этапы имеют схожую структуру, но каждый использует различные логические функции. Обозначение H на рис. В.4 означает функцию хеширования, выполняемую модулем. Обработка 512-битового блока и 160-битового профиля сообщения завершается обновлением содержания 160-битового буфера профиля. После обработки блока содержимое буфера профиля изменится. После того, как обработаны все L 512-битовых блоков на выходе L-этапа образуется 160-битовый профиль сообщения.

В.3.2.2. Применение SHA-1 и RSA для создания ЭЦП

На практике часто целостность сообщения важна для пользователей, а секретность сообщения значения не имеет. На рис. В.5 показана схема передачи открытого сообщения Бобу с использованием хеширования по стандарту SHA-1 и криптографии с открытым ключом. Открытое сообщение P обрабатывается алгоритмом SHA-1, на выходе получается 160-битовый профиль сообщения. Этот профиль сообщения подписывается Алисой (закрытым ключом D_A) и отправляется вместе с открытым сообщением Бобу.

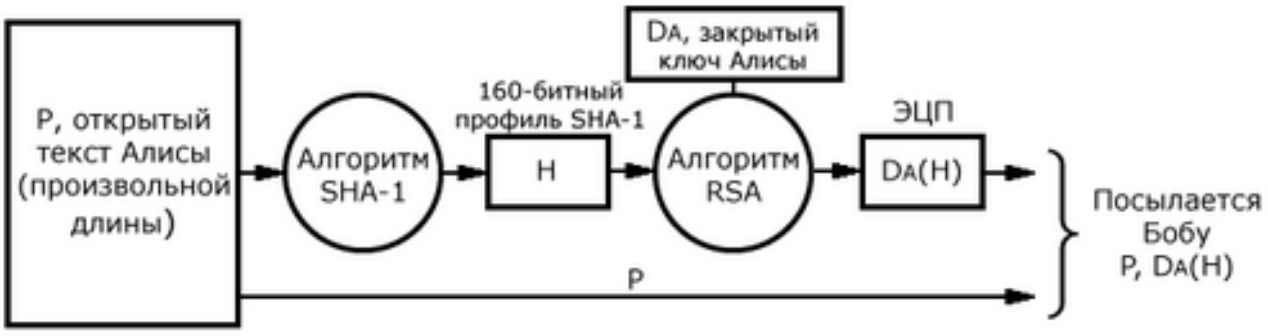


Рис. В.5. Передача открытого сообщения с ЭЦП по стандарту SHA-1

При получении сообщения P вместе с ЭЦП Боб вычисляет хеш-функцию H=h(P) с помощью алгоритма SHA-1 и применяет открытый ключ Алисы к ЭЦП (т.е. $E_A(D_A(H))$ для того, чтобы получить исходный профиль H. Из полученного открытого сообщения Боб формирует его

профиль, т.е. H. Если H и H' совпадают, то это означает, что поступило исходное сообщение P', т.к. злоумышленник не может изменить сообщение P так, чтобы совпали H и H'. Таким образом Боб узнаёт обо всех подменах, которые совершил злоумышленник.

B.3.3. Управление открытыми ключами

B.3.3.1. Угроза «человек посередине»

До сих пор мы полагали, что в асимметричной криптографии открытый ключ подлинный. В действительности шифрование с открытым ключом может быть подвергнуто атаке, которая называется «человек посередине». На рис. B.6 показан способ такого вторжения на примере шифрования/дешифрования сообщения открытым/закрытым ключом получателя.

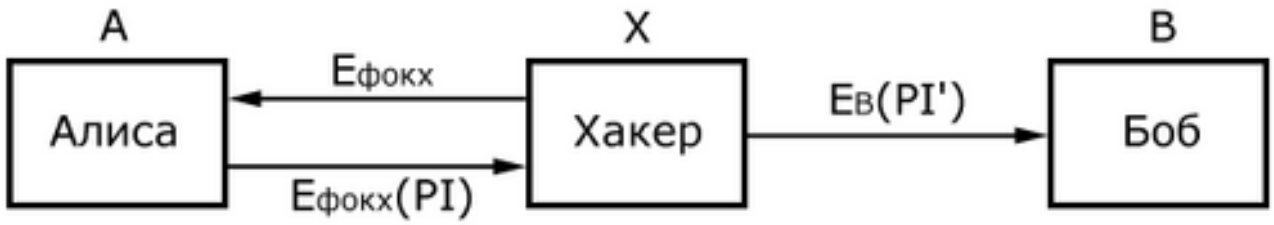


Рис. B.6. Атака «человек посередине»

Хакер посылает Алисе фальшивый открытый ключ $E_{ФОКХ}$, который она получает вместо открытого ключа Боба. Если, например, открытые ключи Алисы и Боба хранятся на сайтах, то хакер пересылает им фальшивую страницу.

Алиса отправляет Бобу сообщение PI, зашифрованное открытым ключом хакера $E_{ФОКХ}$, т.е. сообщение Ефокх(PI). Хакер дешифрирует своим закрытым ключом $D_{фзкх}$, т.е. $PI = D_{фзкх}(E_{фокх}(PI))$. После того, как хакер прочтет сообщение PI от Алисы, он изменяет его содержание на PI' и отправляет Бобу, зашифровав его открытым ключом Боба. Боб своим закрытым ключом $D_B(E_B(PI'))$ дешифрирует это искаженное хакером сообщение Алисы PI.

Для упрощения в примере используется передача зашифрованного сообщения, а не зашифрованного общего ключа симметричного шифрования (т.е. передача цифрового конверта).

B.3.3.2. Сертификаты

Для того чтобы противостоять атаке «человек посередине», разработаны так называемые сертификаты открытых ключей, связываемые с каждым пользователем. Сертификаты включают в себя открытый ключ пользователя и выдаются удостоверяющим центром или Центром Сертификации CA (Certification Authority). Главной целью операции

сертификации является обеспечение уверенности получателя сообщения в том, что открытый ключ отправителя подлинный. Для этого отправитель сообщения должен получить сертификат в удостоверяющем центре, который является независимым и он ему доверяет.

В качестве примера рассмотрим такую ситуацию: Боб желает сформировать сообщение, подписав его цифровой подписью с помощью закрытого ключа, и отправляет эти сообщения Алисе и другим лицам. Всем им известен открытый ключ Боба, с помощью которого они должны будут убеждаться, что подпись правильная. Единственное, в чём они не уверены, это в том, что открытый ключ Боба правильный, т.е. не подделан хакером.

Система сертификации открытого ключа действует следующим образом. Боб приходит в Центр Сертификации (ЦС) со сформированным им открытым ключом, а также паспортом или другим удостоверением личности и просит зарегистрировать открытый ключ. ЦС выдаёт ему сертификат, упрощённый пример которого приведён на рис. В.7. Все данные сертификата можно разделить на 2 части:

- набор открытых элементов, включающий открытый ключ пользователя, идентификатор обладателя ключа и другие элементы. Более полный состав элементов сертификата приведён в таблице В.1 настоящего раздела.
- хеш-функция всей информации первой части, зашифрованная закрытым ключом Центра сертификации (т.е. цифровая подпись сертификата)

После этого Боб оплачивает услуги ЦС и получает дискету с сертификатом.

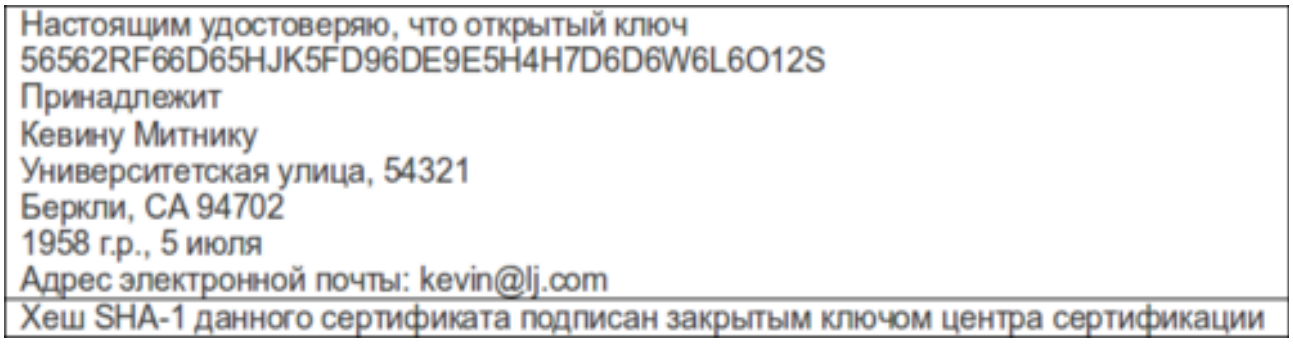


Рис. В.7. Пример сертификата открытого ключа

Основная задача сертификата в связывании открытого ключа с идентификатором владельца этого сертификата (физическим и юридическим лицом). Сертификаты сами по себе не хранятся в тайне и не защищаются. Боб может даже выложить его на свой сайт.

Проверка сертификата Боба осуществляется описанным выше способом сравнения дух профилей: первый профиль определяется с помощью хеш-функции первой части сертификата, а второй профиль с помощью открытого ключа ЦС, т.е. расшифровкой цифровой подписи сертификата. Совпадение профилей означает правильность сертификата.

Что может в данном случае сделать хакер, пытаясь осуществить атаку «человек посередине»? Он может выложить на страницу Боба свой сертификат со своим открытым ключом $E_{фокх}$. Однако Алиса, читая этот сертификат, сразу догадается, что она разговаривает не с Бобом, так как в нём нет идентификатора Боба. Хакер может попробовать и другой способ и заменить в домашней странице Боба его открытый ключ E_B на свой – $E_{фокх}$. Однако хакер не может создать цифровую подпись такого модифицированного сертификата, т.к. он не имеет доступ к закрытому ключу центра сертификации. Эту подделку хакера обнаружит Алиса при попытке проверить полученный сертификат путём сравнения двух профилей, как указано выше.

Сертификат может связывать открытый ключ и с другой информацией. Например, сертификат может накладывать некоторые возрастные ограничения. Допустим, что сайт содержит в сертификате следующую информацию «Данный открытый ключ может быть использован лицами старше 18 лет». Если клиент обеспокоен и хочет убедиться в этом ограничении, он отсылает зашифрованное открытым ключом сертификата случайное число. Если владелец сертификата расшифрует закрытым ключом и отправит это случайное число обратно, то это будет свидетельством того, что владелец сертификата действительно накладывает это ограничение.

Приведём пример другой информации в сертификате. Владелец сертификата указывает в нём список методов, которыми может пользоваться клиент при взаимодействии с этим владельцем. Если владелец сертификата сможет подтвердить это приведённым выше способом, то клиент сможет воспользоваться указанными методами.

В.3.3.3. Стандарт сертификатов X.509

Международный союз ITU-T разработал рекомендацию X.509 [51], включающую стандартизацию сертификата открытого ключа и процедуры аутентификации.

Начиная с 1988 года, вышло 3 версии стандарта. По сути, X.509 – это способ описания сертификатов. Основные поля сертификатов приведены в таблице B.1. Проблема заключается в том, что если Алиса пытается соединиться с bob@mail.com и имеет данные сертификата с именем в формате, для неё вовсе не очевидно, что этот сертификат имеет отношение именно к тому Бобу, который ей нужен.

Таблица B.1. Основные поля сертификатов в стандарте X.509

Поле	Значение
V	Версия X.509
SN	Это число вместе с названием Центра Сертификации однозначно идентифицирует сертификат
AI	Алгоритм подписи сертификата
CA	Имя Центра Сертификации (Удостоверяющего центра)
Ta	Начало и конец периода годности сертификата
A	Идентификатор владельца, ключ которого сертифицируется
Ap	Открытый ключ владельца и идентификатор алгоритма, с которым должен использоваться этот ключ
-	Расширения
-	Подпись сертификата

Стандарт X.509 не требует использовать конкретный алгоритм, хотя и рекомендует RSA.

Стандарт X.509 использует следующую запись:

CA << A >> = CA {V, SN, AI, CA, Ta, A, Ap}-это сертификат пользователя A в центре сертификации CA.

Y << X >> – это сертификат пользователя X, выданный Центром Сертификации Y;

Y{I} – подпись для I, создаваемая объектом Y. Она состоит из I и добавленного зашифрованного профиля I.

Центр сертификации подписывает сертификат своим закрытым ключом. Пользователь, зная открытый ключ ЦС, может удостовериться, что подписанный ЦС сертификат подлинный. Сертификат пользователя, создаваемый Центром Сертификации, имеет следующие характеристики:

- любой пользователь, имеющий открытый ключ Центра Сертификации, может восстановить сертифицированный открытый ключ пользователя;
- никто, кроме Центра Сертификации, не может изменить сертификат без того,

чтобы это было обнаружено.

Поскольку сертификаты фальсифицировать невозможно, их можно разместить в каталоге без применения специальных средств защиты. Если все пользователи используют один ЦС, это означает общее доверие данному Центру Сертификации. Тогда сертификаты пользователей могут размещаться в одном каталоге, доступном всем. Кроме того, любой пользователь может передать свой сертификат другому пользователю непосредственно. В любом случае, если В имеет сертификат А, то В может быть уверен в том, что сообщения, которые он шифрует открытым ключом А, будут защищены от прочтения, а сообщения, подписанные закрытым ключом А, - от фальсификации.

В большом сообществе пользователей обращения всех пользователей к одному и тому же Центру Сертификации практически невозможно. Поскольку сертификаты подписываются Центром Сертификации, каждый пользователь должен иметь собственный экземпляр открытого ключа Центра Сертификации, чтобы проверять подписи. Этот открытый ключ должен быть доставлен каждому пользователю абсолютно защищённым способом (обеспечивающим целостность и аутентичность), чтобы пользователь имел полную уверенность в поступающих сертификатах. Таким образом, при большом числе пользователей может оказаться более удобным иметь ряд ЦС, каждый из которых должен будет защищённым способом доставить открытый ключ некоторой части пользователей.

Предположим, что А получает сертификат от Центра Сертификации X1, а В – от X2. Если пользователю А не был представлен открытый ключ X2 (E_{X2}), то сертификат В ($E_B…D_{X2}(E_B)$), выданный Центром Сертификации X2, окажется для А бесполезным. Пользователь А сможет прочитать сертификат В, но не сможет проверить подпись. Однако, если два Центра Сертификации по какой-то защищённой схеме обменялись своими открытыми ключами, то следующая процедура открывает для А возможность получить открытый ключ В.

На рис. В.8 приведена такая цепочка из двух Центров Сертификации.

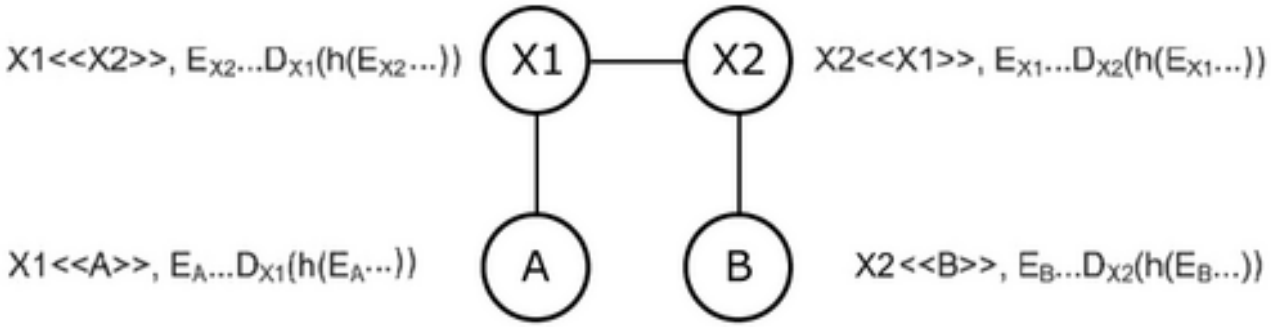


Рис. В.8. Цепочка из двух центров сертификации

Покажем, каким образом пользователь А использует цепочку сертификатов, чтобы получить открытый ключ пользователя В. В обозначениях X.509 эта цепочка записывается в виде X1<<X2>>X2<<B>>.

Этап 1. Пользователь А получает из каталога сертификат X2, подписанный X1 (X1 <<X2>>, т.е. $E_{X2}…D_{X1}(h(E_{X2}))$. Поскольку А с уверенностью знает открытый ключ X1, из полученного сертификата пользователь А сможет извлечь открытый ключ X2 (E_{X2}) и проверить его с помощью подписи, которая была создана X1 для этого сертификата.

Этап 2. Затем А снова обращается к каталогу и получает сертификат В, подписанный X2 (X2<< B >>). Поскольку теперь пользователь А имеет экземпляр открытого ключа X2 (E_{X2}), пользователь А может проверить подпись и получить открытый ключ В.

Точно также В может получить открытый ключ А, но по обратной цепочке:

X2<<X1>>X1<<A>>.

В цепочке может участвовать любое число центров сертификации. Цепочка из N элементов будет иметь следующий вид:

$X1<<X2>>X2<<X3>>…X_N<<B>>$

В этом случае пара центров сертификации в каждом звене (Xi, Xi+1) должна иметь уже готовые сертификаты друг для друга. Все сертификаты Центров Сертификации должны размещаться в каталоге, а пользователю необходимо знать, как они связаны, чтобы проследовать по подходящему маршруту к нужному сертификату открытого ключа другого пользователя.

На рис. В.9 показан гипотетический пример такой иерархии.

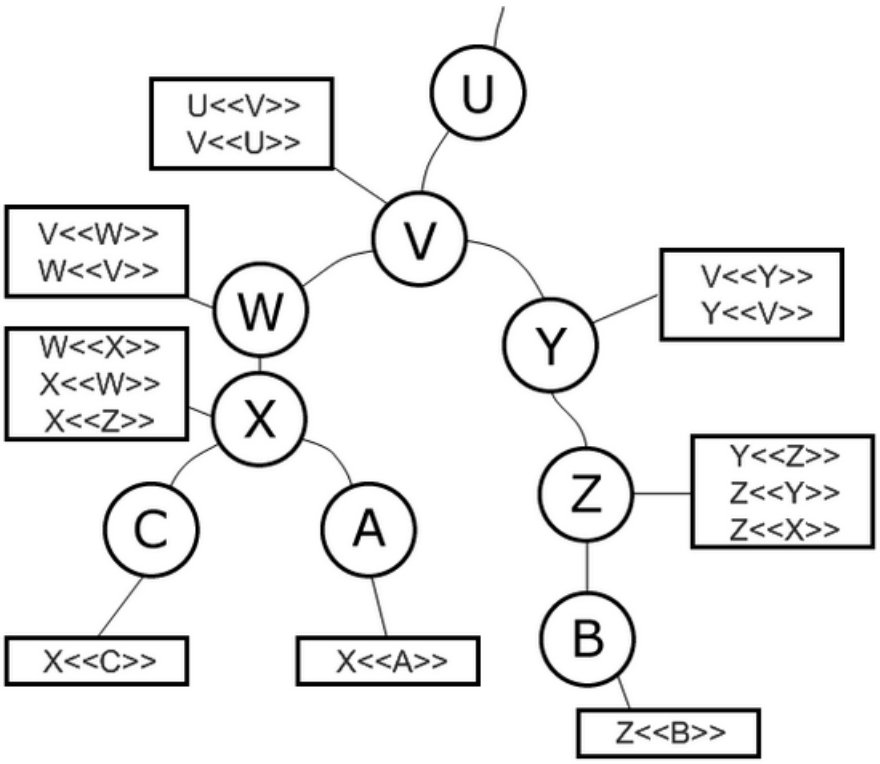


Рис. В.9. Гипотетический пример иерархии Центров Сертификации

Соединённые окружности обозначают иерархически связанные Центры Сертификации, а в указанных рядом прямоугольных блоках приводятся сертификаты, имеющиеся в каталоге соответствующего Центра Сертификации. Каталог Центра Сертификации включает 2 типа сертификатов:

- прямые сертификаты. Сертификаты X, выданные другими Центрами Сертификации;
- возвратные сертификаты. Сертификаты, выданные для сертификации других Центров Сертификации.

В данном примере пользователь A может запросить следующие сертификаты из каталога, чтобы построить сертификационный маршрут к B:

X<<W>>W<<V>>V<<Y>>Y<<Z>>Z<<B>>

Получив эти сертификаты, пользователь A сможет развернуть сертификаты по маршруту один за другим и восстановить надёжный экземпляр открытого ключа B. Используя этот открытый ключ, A сможет посылать B шифрованные сообщения. Если же A понадобится получать шифрованные сообщения от B, то B потребуется открытый ключ A, который может

быть получен по следующей цепочке сертификатов:

Z<<Y>>Y<<V>>V<<W>>W<<X>>X<<A>>
Пользователь B может получить этот набор сертификатов другим способом, если пользователь A включил этот набор в своё исходное сообщение (например, в X включить сертификат X<<Z>>, а в Z включить сертификат Z<<X>>.

Приведённые Центры Сертификации (или удостоверяющие центры), сами сертификаты и каталоги хранения сертификатов объединены в так называемую инфраструктуру систем с открытыми ключами PKI (Public Key Infrastructure).

B.3.3.3.1. Пример проверки подлинности открытого ключа с помощью цепочки сертификатов

Рассмотрим проверку абонентом A открытого ключа абонента B и на примере инфраструктуры PKI, состоящей из цепочки трёх Центров Сертификации ЦС1, ЦС2 и ЦС3 (рис. B.10). Для этого абонент A получает:

- сертификат 1 абонента B, выданный ЦС3

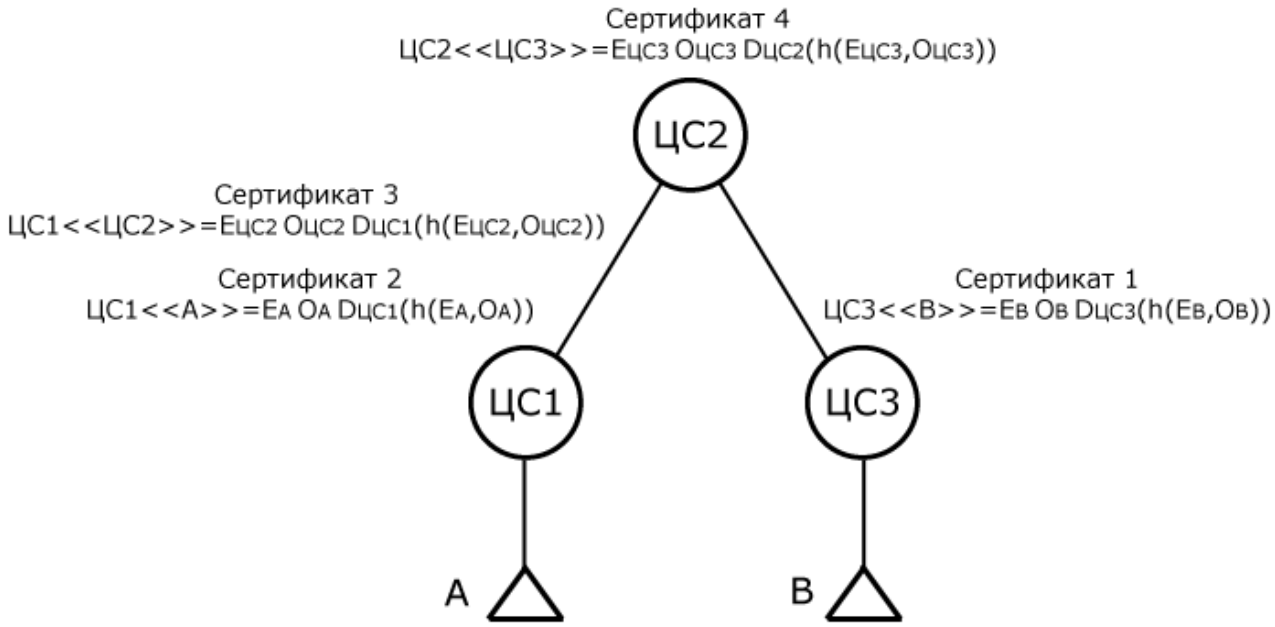


Рис. B.10. Пример проверки с помощью сертификатов абонентом A открытого ключа абонента B

ЦС1<<В>>=ЕвОвDцс3
(h(Ев,Ов)), где
Ев – открытый ключ абонента В;
Ов – часть сертификата абонента В, кроме открытого ключа Ев и цифровой подписи;
Dцс3(h(Ев,Ов)) – цифровая подпись сертификата В.

Абонент А не может быть уверен в подлинности открытого ключа ЕВ, так как не имеет подлинного открытого ключа ЦС3 (т.е. ЕЦС3), который позволяет проверить подлинность цифровой подписи в полученном сертификате. Для того, чтобы проверить эту подпись, абонент А получает ещё 2 сертификата:

- сертификат 3 ЦС2, выданный ему ЦС1.

ЦС1<<ЦС2>> =ЕЦС2ОЦС2DЦС1
(h(ЕЦС2,ОЦС2)), где
ЕЦС2 – открытый ключ ЦС2;
ОЦС2 – часть сертификата ЦС2, кроме ЕЦС2 и цифровой подписи;
DЦС1(h(ЕЦС2,ОЦС2)) – цифровая подпись сертификата ЦС2.

- сертификат 4 ЦС3, выданный ему ЦС2.

ЦС2<<ЦС3>> =ЕЦС3ОЦС3DЦС2
(h(ЕЦС3,ОЦС3)), где
ЕЦС3 – открытый ключ ЦС3;
ОЦС3 – часть сертификата ЦС3, кроме ЕЦС3 и цифровой подписи;
DЦС2(h(ЕЦС3,ОЦС3)) – цифровая подпись сертификата ЦС3.

Сертификат абонента А получен в ЦС1, поэтому ему известен открытый ключ ЦС1, т.е. ЕЦС1. С помощью этого ключа, проверив подпись в сертификате 3 ЦС2, он убеждается в подлинности открытого ключа ЕЦС2. С помощью ключа ЕЦС2, проверив подпись сертификата 4 ЦС3, абонент А убеждается в подлинности открытого ключа ЕЦС3. С помощью ключа ЕЦС3, проверив подпись сертификата 1, абонент А убеждается в подлинности открытого ключа абонента В. В соответствии с принятым обозначением в рекомендации Х.509) соответствующая цепочка сертификатов имеет следующий вид

ЦС1<<ЦС2>>ЦС2<<ЦС3>> ЦС3<<В>>

Аналогичным образом может быть с помощью соответствующих сертификатов проведена проверка абонентом В открытого ключа абонента А. В этом случае цепочка сертификатов имеет следующий вид

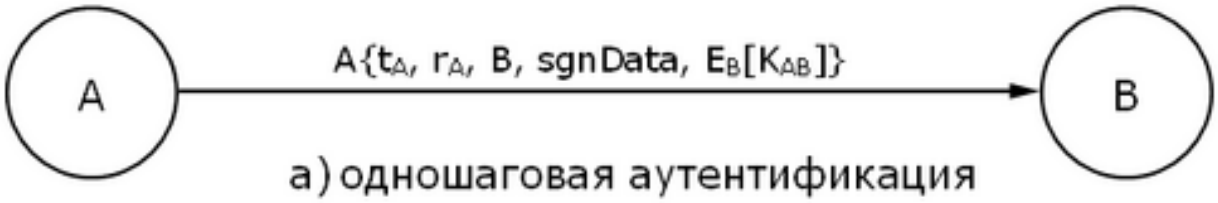
ЦС3<<ЦС2>>ЦС2<<ЦС1>> ЦС1<<А>>

В.3.3.3.2. Процедуры стандарта X.509 аутентификации сообщений и рассылка общих ключей симметричного шифрования

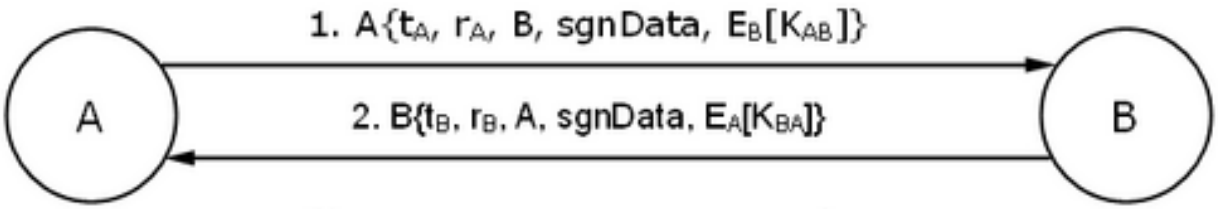
В настоящем разделе приводятся три альтернативные процедуры аутентификации, изложенные в стандарте ITU-T X.509. Шифрование с открытым ключом, кроме создания ЭЦП (что обеспечивает аутентификацию, целостность данных и неотказуемость) используется также для рассылки общих ключей симметричного шифрования.

Схемы всех трех процедур аутентификации X.509 показаны на рис. В.11. Процедуры аутентификации X.509 включают аутентификацию источника сообщения и целостность самого сообщения. Значение внутри фигурных скобок включает набор указанных значений и зашифрованная закрытым ключом отправителя хеш-функция этого набора, т.е. цифровая подпись. Предполагается, что каждая из двух сторон (А и В) проверила подлинность открытого ключа с помощью сертификатов.

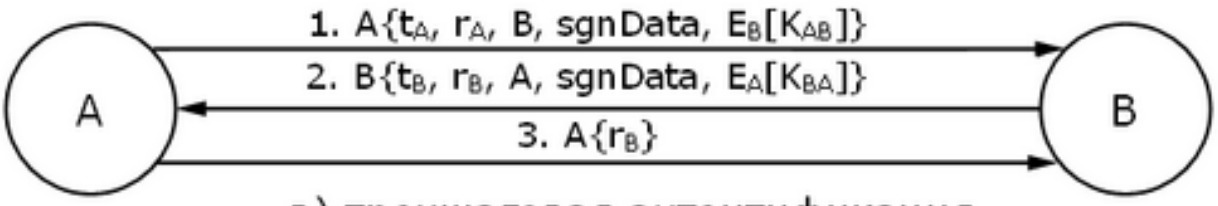
Рис. В.11. Процедура аутентификации X.509



а) одношаговая аутентификация



б) двухшаговая аутентификация



в) трехшаговая аутентификация

Одношаговая аутентификация

Одношаговая аутентификация предполагает передачу одного сообщения от одного пользователя А к другому В, которое устанавливает:

- Аутентичность (подлинность) А и то, что сообщение было создано А.
- Сообщение предназначалось для В.
- Целостность сообщения и защиту от угрозы «повтор».

Кроме этого процедура позволяет передать пользователю В общий ключ симметричного шифрования, сгенерированный пользователем А. Заметим, что данная процедура устанавливает только подлинность источника, но не подлинность получателя. Сообщение должно включать штамп даты-времени t_A, оказию r_A и идентификатор пользователя В и должно быть подписано с использованием закрытого ключа А. Штамп даты-времени складывается из необязательного указываемого времени выдачи и времени окончания срока действия. Это устраняет возможность необоснованной задержки сообщения. Оказию (случайное число r_A) можно использовать для того, чтобы обнаружить атаку «повтор». Значение для оказии должно быть уникальным на протяжении всего срока действия сообщения. Например, В может сохранять значения оказии до истечения срока их действия и отвергать любые новые сообщения с повторяющимися значениями оказии.

В рамках только аутентификации сообщение может использоваться просто для того, чтобы предъявить сертификаты пользователю В. Но сообщение может включать еще и сопровождающую информацию. Эта информация (sgnData) содержится в области действия подписи, что гарантирует ее достоверность и целостность. В состав sgnData может входить информация:

- о ключах сертификации (например, о сроке использования закрытого ключа, т.к. в некоторых случаях он меньше срока использования открытого ключа);
- о политике сертификации. Это расширение предлагает список политик, распознаваемых сертификатом, а также дополнительную уточняющую информацию;
- о субъекте сертификации и центра сертификации (например, альтернативные имена ЦС);
- об ограничении (например, ограничение на длину маршрута).

Как видно из рис. Г.3, а сертификат можно использовать для передачи пользователем А пользователю В общего ключа КАВ симметричного шифрования, зашифровав его предварительно открытым ключом получателя – ЕВ[КАВ]. Этот ключ расшифровывается с помощью закрытого ключа получателя – DB(ED[KAB]).

Двухшаговая аутентификация

Помимо трех указанных выше элементов аутентификации двухшаговая аутентификация является взаимной. По сравнению с одношаговой аутентификацией она позволяет дополнительно:

- сформировать общий ключ симметричного шифрования из двух общих ключей, полученных на каждом шаге аутентификации (КАВ и КВА);
- обмениваться сопровождающей информацией, целостность которой защищена с помощью ЭЦП;
- за счет включения штампа даты-времени сохранить значение оказии (оклика) в течение определенного времени;

Двухшаговая аутентификация, таким образом, позволяет обеим взаимодействующим сторонам проверить аутентичность друг друга.
Ответное сообщение включает оказию А, подтверждающую ответ. Оно также включает

штамп даты-времени и оказию, генерируемую стороной B. Как уже отмечалось выше, сообщение может включать подписанную дополнительную информацию и общий ключ симметричного шифрования, зашифрованный открытым ключом A ($E_A[K_{BA}]$). Ключ K_{BA} позволяет осуществить пересылку шифрованного сообщения абоненту B.

Трёхшаговая аутентификация

При трёхшаговой аутентификации требуется переслать от A к B еще одно сообщение, которое должно содержать подписанную копию оказии r_B. Такая форма сообщения выбирается потому, что проверять штамп даты-времени необходимости нет: обе оказии возвращаются назад другой стороной, а поэтому каждая из сторон имеет возможность обнаружить по значению возвращаемой оказии признаки атаки воспроизведения. Такой подход требуется, когда синхронизация часов невозможна.

ПРИЛОЖЕНИЕ Г. Аутентификация

Аутентификация источника сообщений и аутентификация сообщений (т.е. одновременно подлинности источника сообщений и целостности сообщений) является одной из важнейших функций сетевой защиты. В предыдущем Приложении В приводится описание механизма аутентификации сообщений с помощью электронно-цифровой подписи, основанной на шифровании с открытым ключом.

В настоящем Приложении описываются следующие механизмы аутентификации в сетях связи с использованием шифрования с общим ключом и без шифрования:

- механизм аутентификация источника сообщений по протоколу ОКЛИК-ОТЗЫВ, использующий шифрование с общим ключом;
- механизм аутентификации сообщений с с помощью кода аутентичности сообщения MAC, использующий шифрование с общим ключом без дешифрования;
- механизм аутентификации сообщений по протоколу HMAC без использования шифрования;

Г.1. Аутентификация по протоколу ОКЛИК-ОТЗЫВ

На рис. Г.1 приведена двухпроходная аутентификация по протоколу ОКЛИК-ОТЗЫВ пользователя В аутентифицирующей стороной А.

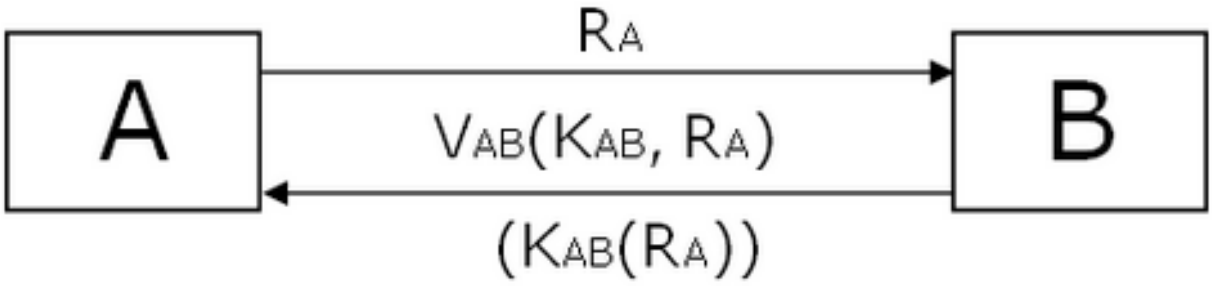


Рис. Г.1. Двухпроходная аутентификация В аутентифицирующей стороной А по протоколу ОКЛИК-ОТЗЫВ

Принятые обозначения:

- RA – случайное число, сгенерированное аутентифицирующей стороной А (оклик);
- VAB = f (KAB, RA) – зашифрованное значение RA с помощью симметричного шифрования с использованием общего ключа KAB в А и В.

Приведем последовательность операций.

- Аутентифицирующая сторона А отправляет В сгенерированное им случайное число RA (оклик);
- Аутентифицируемая сторона В отправляет отзыв VAB, как функция KAB и RA.
- Аутентифицирующая сторона расшифровывает полученный отзыв VAB, получает RA и сравнивает его с отправленным значением RA.
- Аутентификация успешная, если оба значения совпадают. Этот протокол защищает от угрозы «повтор» из-за малой вероятности совпадения случайного числа, созданного злоумышленником, со значением RA.

Г.2. Аутентификация с помощью кода аутентичности сообщения

Метод аутентификации с помощью кода аутентичности сообщения MAC (Message Authentication Code) основан на присоединении к сообщению небольшого блока данных. При этом предполагается, что две участвующие в обмене данными стороны (допустим А и Б) используют общий секретный ключ KАБ. Чтобы послать сообщение М адресату Б, отправитель А вычисляет код аутентичности сообщения как функцию сообщения и ключа: MACМ=F(KАБ,M). Сообщение с добавленным к нему значением MAC, полученное в результате шифрования с общим ключом, пересылается адресату. Получатель выполняет аналогичные вычисления с пришедшим сообщением, используя тот же секретный ключ, и получает свое значение MAC. Вычисленное значение MAC сравнивается с пришедшим вместе с сообщением. Так как секретный ключ знает только получатель и отправитель, то если пришедшее значение MAC совпадает с вычисленным получателем, то можно утверждать:

- подлинность источника сообщения;
- целостность полученного сообщения.

В системах связи используются разные алгоритмы шифрования. Например, алгоритм DES

используется для шифрования сообщения, а определённое число последних битов зашифрованного сообщения (16 или 32) используются в качестве MAC. В сети сотовой связи третьего поколения UMTS используется алгоритм шифрования KASUMI в соответствии со стандартом 3GPP TS.35.202 [83,84].

Г.3. Аутентификация сообщений на основе протокола HMAC

Изложенный в предыдущем Приложении В метод аутентификации сообщений с использованием шифрования с открытым ключом имеет большое достоинство: не требуется доставки секретного ключа симметричного шифрования сообщающимся сторонам. Однако имеются причины в использовании методов аутентификации, позволяющих избежать шифрования:

- алгоритм шифрования работает довольно медленно;
- алгоритмы шифрования могут быть защищены патентами.

Например, алгоритм RSA шифрования с открытым ключом запатентован, и поэтому на использование подобных алгоритмов требуются лицензии, что выливается в дополнительные расходы [9].

На рис. Г.2 показан принцип аутентификации сообщений с помощью функции хеширования, не используя при этом шифрования.

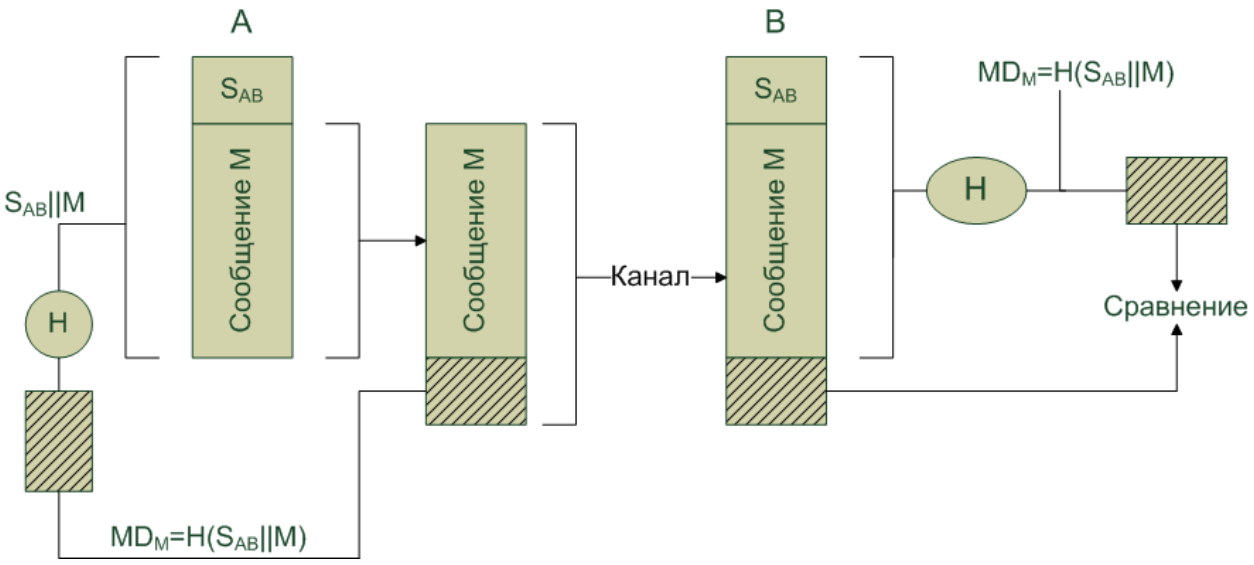


Рис. Г.2. Принцип аутентификации сообщения
с помощью функции хеширования (без использования шифрования)

Программные библиотеки для криптографических функций хеширования доступны.

Для криптографических функций хеширования нет ограничений на экспорт.

Эта технология аутентификации предполагает, что сообщающиеся стороны А и В имеют известное только им общее значение Sав. Перед посылкой стороне В сообщения М требующая аутентификации сторона А вычисляет функцию хеширования Н для конкатенации этого секретного значения и текста сообщения: MDм = Н (Sав || М). Затем М || MD_M пересылается стороне В. Поскольку сторона В имеет значение Sав, она может вычислить Н (Sав || М) и проверить соответствие вычисленного значения полученному значению MDм. Поскольку само секретное значение Sав с сообщением не пересылается, у злоумышленника нет возможности модифицировать перехваченное сообщение MDм. Злоумышленник не может генерировать фальшивое сообщение, поскольку не знает секретное значение Sав.

Одним из наиболее широко используемых протоколов, работающих по указанному принципу без использования шифрования, является алгоритм, называемый HMAC (Hashed Message Authentication Code - код идентификации хешированного сообщения).

Приведем алгоритм HMAC. Особенностью HMAC является использование вложенных хеш-операций ключей, одна внутри другой.

Эта идея основана на использовании двух дополняющих значений (pad values), одно из которых называется внутренним (ipad), а другое внешним (opad), которые применяются в хеш-алгоритме Н, выполняемом над сообщением М, с использованием секретного ключа К.

HMAC (К, М) = H[(K^+ XOR opad)||H[(K^+ XOR ipad)|| M]],

где b - число байт в блоке, ipad = байт 36 (шестнадцатеричный), повторенный b раз, opad = байт 5С (шестнадцатеричный), повторенный b раз. Это интерпретируется следующим образом:

- Добавить нули в конец К для того, чтобы получить строку длиной b байт (например, если К имеет длину 20 байт и b = 64, то к K^+ будет добавлено 44 нулевых байта).
- Операция «исключающее ИЛИ» XOR (по модулю 2) проводится над полученной в первом шаге строкой и ipad.
- Входной поток данных М присоединяется (операция конкатенации) к результату операции в шаге 2.
- Применить Н к потоку данных, полученных в шаге 3.
- Операция «исключающее ИЛИ» проводится над полученной в первом шаге строкой и opad.
- Результат шага 4 присоединяется к результату шага 5.

- Применить H к потоку данных, полученных в шаге 6, и вывести результат.

Алгоритм HMAC принят как обязательный для реализации аутентификации сообщений в протоколе IPSec, выполняющем защиту на межсетевом уровне IP-сети.

ПРИЛОЖЕНИЕ Д. Формирование общего секретного ключа с помощью метода Диффи-Хеллмана

В приложении В приведено описание распределение ключей (обмен общими секретными ключами) и защита с помощью сертификатов от угрозы «человек посередине».

В настоящем приложении, посвященном методу Диффи-Хеллмана [9], изложен другой способ создания общего секретного ключа для взаимодействующих абонентов сети. Приводится пример угрозы «человек посередине», для защиты от которых также служат сертификаты. Этот метод используется для управления ключами протоколом защиты транспортного уровня TLS (глава 13).

Д.1. Дискретный логарифм

В основу алгоритма Диффи-Хеллмана положена трудность вычисления дискретных логарифмов. Определим понятие дискретного логарифма.

Сначала определяется первообразный корень α простого числа q, как число, степени которого по модулю q $(\alpha \bmod q, \alpha^2 \bmod q, \alpha^3 \bmod q, \ldots \alpha^{q-1} \bmod q)$, составляют полный набор целых чисел от 1 до ($q-1$). Например, если первообразный корень $\alpha = 7$, а $q = 11$, тогда для полного набора i от 1 до 10 (т.е. $q-1$) $b = \alpha^i \bmod q = 7^i \bmod 11$ (принимает значения от 1 до 10.

В нижеследующей таблице приведены результаты вычислений, подтверждающие то, что α - первообразный корень числа q.

i	1	2	3	4	5	6	7	8	9	10
$b = 7^i \bmod 11$	7	5	2	3	10	4	6	9	8	1

С целью упрощения вычислений воспользуемся следующим правилом арифметики в остаточных классах (классах вычетов) $a^{n_1+n_2} \bmod p = \left[\left(a^{n_1} \bmod p\right)\left(a^{n_2} \bmod p\right)\right] \bmod p$

Показатель степени i называется дискретным логарифмом. При больших значениях первообразного корня α и простого числа q (порядка 512бит) по известному значению b

вычисление дискретного логарифма становится практически неразрешимой задачей.

Д.2. Формирование общего ключа симметричного шифрования

На рис. Д.1 приведено формирование общего ключа симметричного шифрования.

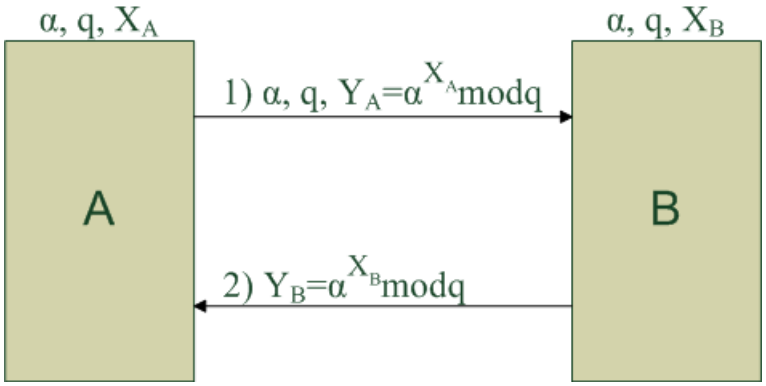


Рис. Д.1. Формирование общего ключа симметричного шифрования

Как видно из рис. Д.1., пользователь А определяет параметры и первообразный корень α простого числа q. Оба эти числа в открытом виде отправляют пользователю B в сообщении 1. На α накладывается условие: $(\frac{\alpha-1}{2})$ должно быть простым числом. Кроме этого на q накладываются некоторые дополнительные условия. Значения α и q могут быть определены пользователем B и в открытом виде отправлены пользователю A.

Пользователь A выбирает случайное целое число $X_A < q$ и вычисляет открытый ключ $Y_A = \alpha^{X_A} \text{ m} \quad q$. Аналогично пользователь В выбирает случайное целое число $X_B < q$ и вычисляет открытый ключ $Y_B = \alpha^{X_B} \text{ m} \quad q$. Значения X_A и X_B являются большими числами (например, 512-разрядными), и они сохраняются пользователями в секрете. Значения Y_A и Y_B (открытые ключи) свободно доступны другой стороне и поэтому передаются в сообщениях 1 и 2. Пользователь A вычисляет общий ключ $K_A = (Y_B)^{X_A} \text{ m} \quad q$, а пользователь B по формуле $K_B = (Y_A)^{X_B} \text{ m} \quad q$.

Покажем, что оба ключа K_A и K_B равны. Воспользуемся для этого арифметикой в остаточных классах.

$$K_A = (Y_B)^{X_A} \bmod q = (\alpha^{X_B} \bmod q)^{X_A} \bmod q = (\alpha^{X_B})^{X_A} \bmod q =$$

$$= \alpha^{X_B X_A} \bmod q = (\alpha^{X_A})^{X_B} \bmod q = (\alpha^{X_A} \bmod q)^{X_B} \bmod q = (Y_A)^{X_B} \bmod q = K_B$$

Таким образом, у пользователей A и B общий секретный ключ $K_A = K_B$.

Как видно из рис. Д.1, хотя величины α, q и Y_A известны (из сообщения), злоумышленнику вычислить дискретный логарифм X_A из $Y_A = \alpha^{X_A} \bmod q$ на сегодняшний день практически невозможно. Поэтому оказывается невозможным злоумышленнику вычислить общий секретный ключ $K_A = (Y_B)^{X_A} \bmod q$.

Аналогично злоумышленнику невозможно вычислить дискретный логарифм X_B из $Y_B = \alpha^{X_B} \bmod q$ (при известных значениях α, q, Y_B). Поэтому оказывается невозможным вычислить общий секретный ключ $K_B = (Y_A)^{X_B} \bmod q$.

Пример

Для иллюстрации формирования общего секретного ключа с помощью алгоритма Диффи-Хеллмана выберем нереально небольшие значения $\alpha = 7$ и $q = 71$.

Пользователи А и В выбирают также нереально небольшие значения $X_A = 5$ и $X_B = 12$.

$$Y_A = \alpha^{X_A} \bmod q = 7^5 \bmod 71 = 16807 \bmod 71 = 5$$

$$Y_B = \alpha^{X_B} \bmod q = 7^{12} \bmod 71 = ((7^2 \bmod 71) * (7^5 \bmod 71) * (7^2 \bmod 71)) \bmod 71 = (5 * 5 * 4) \bmod 71 = 100 \bmod 71 = 29$$

Производится обмен значениями Y_A и Y_B между пользователями.

Определяем значения ключей K_A и K_B.

$$K_A = (Y_B)^{X_A} \bmod q = 29^5 \bmod 71 = 3$$

$$K_B = (Y_A)^{X_B} \bmod q = 5^{12} \bmod 71 = [(5^4 \bmod 71)^3] \bmod 71 = 3$$

Таким образом, независимо друг от друга пользователи А и В определили общий секретный ключ $K_A = K_B = 3$.

Пользователь В получает сообщение 1 со значениями $\alpha = 7$, $q = 71$ и $Y_A = 4$.

Злоумышленнику путем полного перебора для таких небольших чисел удастся определить дискретный логарифм X_A из выражения $4=7^{X_A} \bmod 7$ (т.е. $X_A = 5$). Для значений α, q, Y_A, в несколько сотен бит каждый, эта задача определения X_A неразрешима.

Д.3. Уязвимость алгоритма Диффи-Хеллмана к атаке «человек посередине»

Приведенный алгоритм Диффи-Хеллмана так же, как и использование открытого и закрытого ключа в криптографии с открытым ключом позволяет использовать созданные секретные ключи для симметричного шифрования сообщений пары пользователей сети связи. Если не использовать эти алгоритмы, то каждому абоненту потребуется содержать очень большое число ключей, равное числу сочетаний $C_N^2 = N*(N-1)/2$, где N - число абонентов в сети. Если абонентов 10 тысяч, то ключей должно быть $5*10^7$. Снабжение таким большим количеством ключей становится очень громоздкой и дорогостоящей задачей. Открытое распространение параметров и вычисление ключей позволило решить эту проблему.

Однако по сравнению с созданием общего ключа симметричного шифрования с помощью шифрования с открытым ключом (приложение Г, раздел Г.3) алгоритм Диффи-Хеллмана не обеспечивает защиты от угрозы «человек посередине».

Когда пользователь В получает сообщение 1 (рис. Д.1). Как он сможет удостовериться в том, что оно послано пользователем А, а не злоумышленником? На рис. Д.2 показана атака злоумышленника «человек посередине».

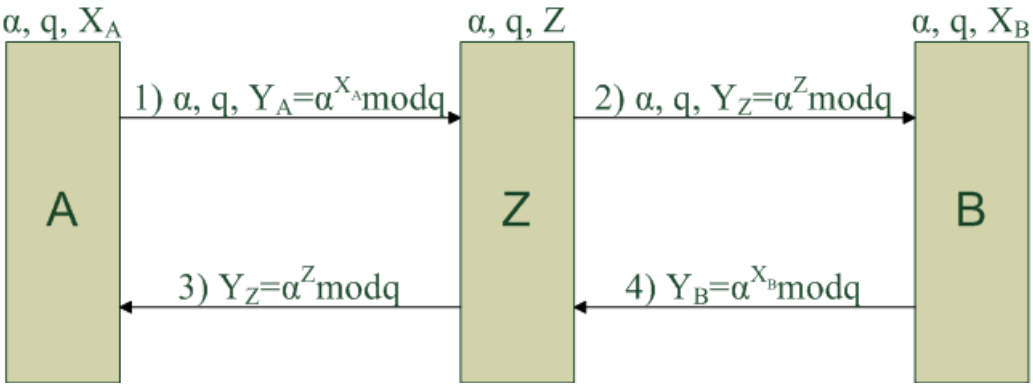


Рис. Д.2. Атака типа «человек посередине»

Пользователь А пересылает пользователю В сообщение 1, которое перехватывает злоумышленник. Злоумышленник выбирает свое секретное значение Z и отправляет пользователю В вместо сообщения 1 сообщение 2, используя правильные открытые α и q,

но вместо Y_A передает свое значение $Y_Z = \alpha^Z \bmod q$. Он также посылает это значение пользователю А (сообщение 3).

Получив сообщение 2, пользователь В отправляет пользователю А сообщение 4, которое перехватывает также злоумышленник.

- Обратите внимание на то, что сообщения 1 и 2 (рис. Д.1) те же самые, что и сообщения соответственно 1 и 4 (рис. Д.2).

В результате атаки между пользователем А и злоумышленником создается один общий ключ симметричного шифрования K_{AZ}, а между пользователем В и злоумышленником создается другой ключ – K_{BZ}. В результате каждое сообщение, посылаемое А, шифрованное ключом K_{AZ}, дешифруется злоумышленником, изменяется, если это нужно злоумышленнику, и отправляется пользователю В, предварительно зашифровав его ключом K_{AZ}. То же самое происходит и в обратном направлении. Пользователи А и В полагают, что у них имеется защищенный канал между ними, в то время, как злоумышленник читает все сообщения и может изменить их по своему усмотрению.

Приведем пример, иллюстрирующий вышесказанное.

Пример

Исходные данные пользователей А и В те же, что и в предыдущем примере (раздел Д.2):

$\alpha = 7,\ q = 71,\ X_A = 5,\ X_B = 12,\ Y_A = 51,\ Y_B = 4.$

Примем, что злоумышленник выбирает свое секретное значение Z=3.

Злоумышленник определяет $Y_Z = \alpha^Z \bmod q = 7^3 \bmod 71 = 5$.

Пользователь А определяет общий ключ со злоумышленником

$$K_A = Y_Z^{X_A} \bmod q = 5^5 \bmod 71 = 29 = 2 \text{ d}$$

Злоумышленник определяет общий ключ с пользователем А

$$K_Z = Y_A^{X_Z} \bmod q = 5^3 \bmod 71 = 92$$

Оба ключа K_{AZ} и K_{ZA} совпадают, и он является общим на участке «пользователь А – злоумышленник».

Пользователь В определяет общий ключ со злоумышленником

$$K_B = Y_Z^{X_B} \bmod q = 5^{12} \bmod 71 = 9(5^3 \bmod 17)^4 \bmod 71 = 14^4 \bmod 71 = 76$$

Злоумышленник определяет общий ключ с пользователем В

$$K_Z = Y_B^Z \bmod q = 4^3 \bmod 71 = 6$$

Оба ключа K_{BZ} и K_{ZB} совпадают, и он является общим на участке «пользователь В – злоумышленник».

Оглавление

Значения общих ключей злоумышленника с пользователем А и с пользователем В разные, что и позволяет злоумышленнику осуществлять нарушения.

В главе 13 приводится описание протокола TLS обеспечения ИБ на транспортном уровне TCP/IP, использующего защиту метода Диффи-Хеллмана от угрозы «человек посередине». При этом могут быть использованы следующие механизмы защиты открытых параметров (первообразный корень, простое число и открытый ключ):

- передача в составе сертификата;
- шифрование открытым ключом получателя по алгоритму RSA;
- подпись закрытым ключом отправителя по алгоритму RSA.

ПРИЛОЖЕНИЕ Е. Протокол ИБ прикладного уровня PGP

Настоящее приложение посвящено более детальному изложению следующих функций механизмов безопасности протокола **PGP**, которые не были освещены в главе 13:

- пользователь имеет несколько пар открытых/закрытых ключей асимметричной криптографии. Это относится к выполнению правила Кирхгоффа об ограничении времени использования одного и того же ключа путем частой смены его (приложение Б);
- шифрование секретных ключей асимметричной криптографии при хранении в оборудовании.

В настоящем приложении приводится описание алгоритма обеспечения конфиденциальности и аутентификации сообщений электронной почты, реализованного в протоколе PGP (Pretty Good Privacy – достаточная надежная секретность). В настоящем приложении приводится описание алгоритма PGP по обеспечению для одного сообщения и аутентификации и конфиденциальности. В отличие от главы 13 здесь приводится более детальное описание этих алгоритмов, учитывающее указанные выше требования к ключам шифрования. При этом используются следующие обозначения:

– M – открытое сообщение в конечном пункте;

– X – открытое сообщение в оконечном пункте;

– C – сообщение в канале связи;

– K_S - общий (сеансовый) ключ, используемый в схеме симметричного шифрования;

– $E_{KS}[X]$ - шифрование общим (сеансовым) ключом K_S сообщения X;

– $D_{KS}[X]$ - расшифрование общим (сеансовым) ключом K_S сообщения X;

– D_A - закрытый ключ пользователя A, используемый в схеме шифрования с открытым ключом;

– D_B - закрытый ключ пользователя B, используемый в схеме шифрования с открытым ключом;

– E_A - открытый ключ пользователя A, используемый в схеме шифрования с открытым ключом;

– E_B - открытый ключ пользователя B, используемый в схеме шифрования с открытым ключом;

– EP – шифрование в схеме с открытым ключом;

– DP – расшифрование в схеме с открытым ключом;

– EC – шифрование в схеме с общим ключом;

– DC – расшифрование в схеме с общим ключом;

– H – функция хеширования;

– II – конкатенация.

Секретным мы будем называть общий ключ симметричного шифрования, а закрытым и открытым ключами при шифровании с открытым ключом.

.

E1. Криптографические ключи

PGP использует четыре типа ключей: одноразовые общие (сеансовые) ключи симметричного шифрования, открытые ключи, закрытые ключи асимметричной криптографии и парольные ключи схемы симметричного шифрования. В отношении этих ключей алгоритм ИБ выполняет следующие три требования:

– необходимо иметь средства генерирования непредсказуемых секретных ключей;

– желательно, чтобы пользователь имел несколько пар открытых/закрытых ключей. Тогда он сможет время от времени менять пару ключей. Но в результате все сообщения, находящиеся в этот момент в пути следования, окажутся созданными со старым ключом. К тому же получатели будут знать только старый открытый ключ до тех пор, пока не получат новую версию ключа. В дополнение к необходимости время от времени менять ключи пользователь может иметь разные пары ключей для взаимодействия с различными группами получателей или просто для того, чтобы усилить защиту, ограничивая объем материала, шифруемого одним и тем же ключом. При этом теряется однозначность соответствия между пользователями и их открытыми ключами и возникает необходимость в средствах, позволяющих идентифицировать конкретные ключи;

– каждый объект системы PGP должен поддерживать файл собственных пар открытых/закрытых ключей, а также открытых ключей других пользователей, с которыми данный объект взаимодействует.

Шифрование сообщения производится общим (сеансовым) ключом симметричного шифрования. Сгенерированный на одном оконечном пункте этот ключ передается с помощью цифрового конверта противоположному оконечному пункту. Цифровым конвертом является этот ключ, зашифрованный с помощью открытого ключа получателя.

Следовательно, только получатель сможет расшифровать сеансовый ключ, чтобы с его

помощью прочесть сообщение. Если бы каждый пользователь использовал одну пару открытого и закрытого ключей, то получатель сразу бы знал, с помощью какого ключа можно расшифровать секретный ключ – с помощью единственного закрытого ключа получателя. Однако PGP выполняет требование, чтобы пользователь мог иметь много пар открытых/закрытых ключей.

Как в этом случае пользователю узнать, какой из открытых ключей использовался для шифрования секретного ключа? Простейшим решением является передача открытого ключа вместе с сообщением. Получатель мог бы тогда удостовериться, что это действительно один из открытых ключей, а затем продолжить обработку сообщения. Эта схема должна работать, но при этом пересылается слишком много лишних данных. Открытый ключ RSA может иметь длину в сотни десятичных разрядов. Другим решением является связывание с каждым открытым ключом некоторого идентификатора, уникального, по крайней мере, для одного пользователя. Для этой цели вполне подойдет, например, комбинация идентификатора пользователя и идентификатора ключа. Такое решение, однако, порождает проблему управления: идентификаторы ключей должны выбираться и храниться так, чтобы как отправитель, так и получатель смогли установить соответствие между идентификаторами ключей и самими открытыми ключами.

В PGP каждому открытому ключу присваивается идентификатор, который с очень высокой вероятностью должен быть уникальным для данного пользователя. Идентификатор, связываемый с каждым открытым ключом, представляет собой значение, хранящееся в младших 64 разрядах открытого ключа. Это означает, что идентификатор открытого ключа E_A равен $E_A \bmod 2^{64}$. Этой длины достаточно для того, чтобы вероятность дублирования идентификаторов ключей оказалась очень малой.

Идентификатор ключа требуется и для цифровой подписи PGP. Из-за того, что отправитель может воспользоваться одним из нескольких закрытых ключей для шифрования профиля сообщения, получатель должен знать, какой открытый ключ ему следует использовать. Поэтому раздел цифровой подписи сообщения включает 64-битовый идентификатор соответствующего открытого ключа. Получив сообщение, адресат проверяет, соответствует ли идентификатор известному ему открытому ключу отправителя, а затем приступает к проверке подписи.

E2. Общий формат передаваемого сообщения

Теперь, определив понятие идентификаторов, приведем рис. Е.1 общий формат передаваемого сообщения от А к В. Как видно из рисунка, сообщение состоит из трех компонентов: собственно сообщение, цифровая подпись и секретный ключ.

Обозначения:

D_A – шифрование с использованием закрытого ключа пользователя А

E_A – открытый ключ пользователя А

E_B – открытый ключ пользователя В

Ek_s – шифрование с использованием сеансового ключа

ZIP – функция сжатия Zip

R64 – функция преобразования в формат radix-64

Рис. Е.1. Общий формат сообщения PGP (от А к В)

- **Компонент сообщения** включает фактические данные, предназначенные для хранения или передачи, а также имя файла и штамп даты-времени, указывающий время создания сообщения.
- **Компонент подписи** включает следующие элементы.

- Штамп даты-времени. Время создания подписи.

- Профиль сообщения. 160-битовый профиль сообщения, созданный с помощью SHA-1 и зашифрованный с использованием закрытого ключа подписи отправителя. Профиль вычисляется для штампа даты-времени подписи, связанного конкатенацией с порцией данных компонента сообщения. Включение штампа даты-времени подписи в профиль сообщения обеспечивает защиту от атак воспроизведения.
- Идентификатор открытого ключа отправителя. Идентифицирует открытый ключ, который должен использоваться для дешифрования профиля сообщения и, следовательно, идентифицирует закрытый ключ, имеющийся для шифрования профиля сообщения.

Компонент сообщения и необязательный компонент подписи могут быть сжаты с помощью ZIP и зашифрованы с использованием закрытого ключа.

Как видно из рис. Е1 PGP сжимает сообщение после создания подписи, но перед шифрованием. Это оказывается разумным с точки зрения уменьшения объема данных, как при передаче электронной почты, так и при хранении в виде файлов.

Подпись генерируется до сжатия по следующим причинам:

– предпочтительнее подписывать несжатое сообщение, чтобы в будущем иметь возможность хранить сообщение в несжатом виде вместе с подписью. Если подписать сжатый документ, то для проверки необходимо будет, либо хранить сжатую версию сообщений, либо сжимать сообщение для каждой верификации;

– даже при возможности динамически повторно сжимать сообщение для верификации такой подход несет в себе дополнительные трудности из-за самого алгоритма сжатия PGP. Алгоритм сжатия не является детерминированным и различные реализации алгоритма выбирают разные варианты оптимизации соотношения скорости выполнения и сжатия, в результате получаются сжатые файлы разной формы. Применение функции хеширования и создания подписи после сжатия заставило бы во всех реализациях PGP применять один и то же алгоритм сжатия.

В качестве алгоритма сжатия применяется ZIP. Алгоритм основан на том факте, что слова и фразы внутри потока текста, вероятнее всего, повторяются. Когда это имеет место, повторная последовательность может быть заменена более коротким кодом. Программа сжатия находит такие повторения и строит коды прямо по ходу обработки данных, заменяя повторяющиеся последовательности. В дальнейшем коды применяются повторно, чтобы обработать новые последовательности. Алгоритм должен быть определен таким образом, чтобы программа распаковке могла построить правильное отображение кодов в последовательности исходных данных.

- **Компонент сеансового ключа** содержит зашифрованный общий сеансовый ключ и

идентификатор открытого ключа получателя, который использовался отправителем для шифрования данного сеансового ключа.

Как видно из рис. Е1, все сообщение PGP переводится в формат radix-64. При этом производится конвертирование данных в поток печатных символов.

При использовании PGP шифруется, по крайней мере, часть передаваемого блока. Если требуется только цифровая подпись, то шифруется профиль сообщения (с использованием закрытого ключа отправителя). Если используется конфиденциальность, шифруется (с использованием одноразового общего ключа) сообщение и подпись (при наличии последней). Таким образом, часть или весь выходной блок сообщения представляет собой поток произвольных 8-битовых байтов. Однако многие системы электронной почты позволяют использовать только блоки, состоящие из символов текста ASCII. В связи с такими ограничениями PGP поддерживает сервис конвертирования 8-битового двоичного потока данных в поток печатаемых символов ASCII.

Для этого используется схема конвертирования в 64-символьный формат (base-64 или radix-64). Каждая группа из трех байтов двоичных данных преобразуется в четыре символа ASCII, к которым присоединяется контрольная сумма (CRC), позволяющая обнаружить ошибки при передаче данных.

Следует отметить, что алгоритм radix-64 конвертирует входной поток в 64-символьный формат, невзирая на содержимое – даже если ввод уже оказывается текстом ASCII. Таким образом, если сообщение подписано, но не шифруется, и конвертирование применяется по всему блоку, то выходной поток данных будет непонятен случайному наблюдателю, что уже обеспечивает определенный уровень конфиденциальности. В последнем разделе настоящего приложения приводится описание radix-64.

E.3. Связки ключей

Мы видели, что идентификаторы ключей в PGP очень важны, и два идентификатора ключей включаются в любое сообщение PGP, предполагающее конфиденциальность и аутентификацию. Эти ключи необходимо хранить и организовать некоторым стандартизированным образом для эффективного применения всеми сторонами, участвующими в обмене данными. Используемая в PGP схема предполагает создание в каждом узле двух структур данных, из которых одна используется для хранения пар открытых/закрытых ключей данного узла, а другая – для хранения открытых ключей других пользователей, известных данному узлу. Эти структуры данных называются *соответственно связкой закрытых ключей и связкой открытых ключей*.

Общая структура связки закрытых ключей показана на рис. E.2. Связку можно интерпретировать как таблицу, в которой каждая строка представляет одну пару связанных ключей (открытый и закрытый), принадлежащих данному пользователю. Строки состоят из следующих полей:

- Штамп даты-времени. Дата и время создания данной пары ключей.
- Идентификатор ключа. Младшие 64 разряда открытого ключа данной строки.
- Открытый ключ. Открытый ключ данной пары.
- Закрытый ключ данной пары; это поле шифруется.
- Идентификатор пользователя. Обычно здесь размещается адрес электронной почты пользователя.

Связка закрытых ключей (данного пользователя)

Штамп даты-времени	Идентификатор ключа*	Открытый ключ	Шифрованный закрытый ключ	Идентификатор пользователя*
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
T_i	$E_i \bmod 2^{64}$	E_i	$E_{H(P)}[D_i]$	Пользователь i
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

Связка открытых ключей (других пользователей)

Штамп даты-времени	Идентификатор ключа*	Открытый ключ	Идентификатор пользователя*	Подпись (подписи)	Доверие подписи (подписям)
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
T_i	$E_i \bmod 2^{64}$	E_i	Пользователь i		
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

* – поле, используемое для индексации таблицы

Рис. Е.2. Общая структура связок закрытых и открытых ключей

Хотя предполагается, что связка закрытых ключей должна храниться только на машине пользователя, создавшего и владеющего соответствующими парами ключей, и должна быть доступна только этому пользователю, имеет смысл сделать значения закрытых ключей защищенными настолько, насколько это возможно. Соответственно, сам закрытый ключ в открытом виде в связке ключей не хранится, а шифруется с помощью симметричной криптографии.

При этом используется следующая процедура.

1. Пользователь выбирает фразу-пароль, которая будет служить для шифрования закрытых ключей.

2. Когда система с помощью RSA генерирует новую пару связанных ключей (открытый и закрытый), она требует от пользователя указать такую фразу-пароль. Из нее с помощью SHA-1 генерируется 160-битовый хеш-код, а затем пароль удаляется.

3. Система шифрует с помощью симметричной криптографии закрытый ключ D_i, используя 128 бит хеш-кода (P_i) в качестве ключа. Хеш-код затем удаляется, а шифрованный закрытый ключ $E_{H(P_i)}[D_i]$ сохраняется в связке закрытых ключей.

Впоследствии, когда пользователь обратится к связке, чтобы извлечь закрытый ключ, ему придется снова указать фразу-пароль. PGP извлечет шифрованный закрытый ключ, вычислит хеш-код пароля и дешифрует закрытый ключ ключом хеш-кода (128 бит).

Как и в любой, основанной на паролях системе, защищенность всей системы зависит от защищенности пароля.

На рис. Е.2 показана общая структура связки открытых ключей. Эта структура данных позволяет хранить открытые ключи других пользователей, известных данному узлу.

Поясни некоторые поля этой таблицы.

- Штамп даты-времени. Дата и время создания данной записи.
- Идентификатор ключа. Младшие 64 разряда открытого ключа данной записи.
- Открытый ключ. Открытый ключ данной записи.
- Идентификатор пользователя. Определяет владельца данного ключа. С одним открытым ключом можно связать несколько идентификаторов пользователя.

Е.4. Обеспечение ИБ при передаче и приеме сообщений

В настоящем разделе приводится описание алгоритма аутентификации и конфиденциальности ИБ при передаче и приеме сообщений. При этом учитывается использование связки ключей и шифрование/дешифрование ключа симметричной криптографии.

Сначала рассмотрим создание сообщения на передачу (рис. Е.3) и предположим, что сообщение должно быть подписано, и зашифровано. Посылающий сообщение объект А выполняет следующие шаги.

1. Создание подписи сообщения.

- PGP извлекает зашифрованный закрытый ключ отправителя из связки закрытых ключей. Создается хеш-функция фразы пароль, которая служит ключом для того, чтобы с помощью симметричной криптографии DC расшифровать закрытый ключ D_A.

- Создается цифровая подпись сообщения М - $D_A[H(M)]$, где Н(М) - хеш-код этого сообщения М;

2. Шифрование сообщения.

- PGP генерирует секретный общий ключ K_S и шифрует им с помощью симметричной криптографии ЕС сообщение вместе с цифровой подписью - $Ks[M||D_A[H(M)]]$.

- PGP извлекает открытый ключ получателя E_B из связки открытых ключей.

– Создается цифровой конверт $E_B(Ks)$ секретного ключа сообщения Ks.

– В канал абоненту В передается зашифрованное сообщение вместе с цифровой подписью $D_A[H(M)]$ и идентификатором закрытого ключа отправителя А - $E_A mod 2^{64}$, цифровой конверт $E_B(Ks)$ и идентификатор открытого ключа получателя $E_в mod 2^{64}$ т.е. $Ks[[M||D_A[H(M)]]||E_A mod 2^{64}]E_B(Ks)||E_B mod 2^{64}$.

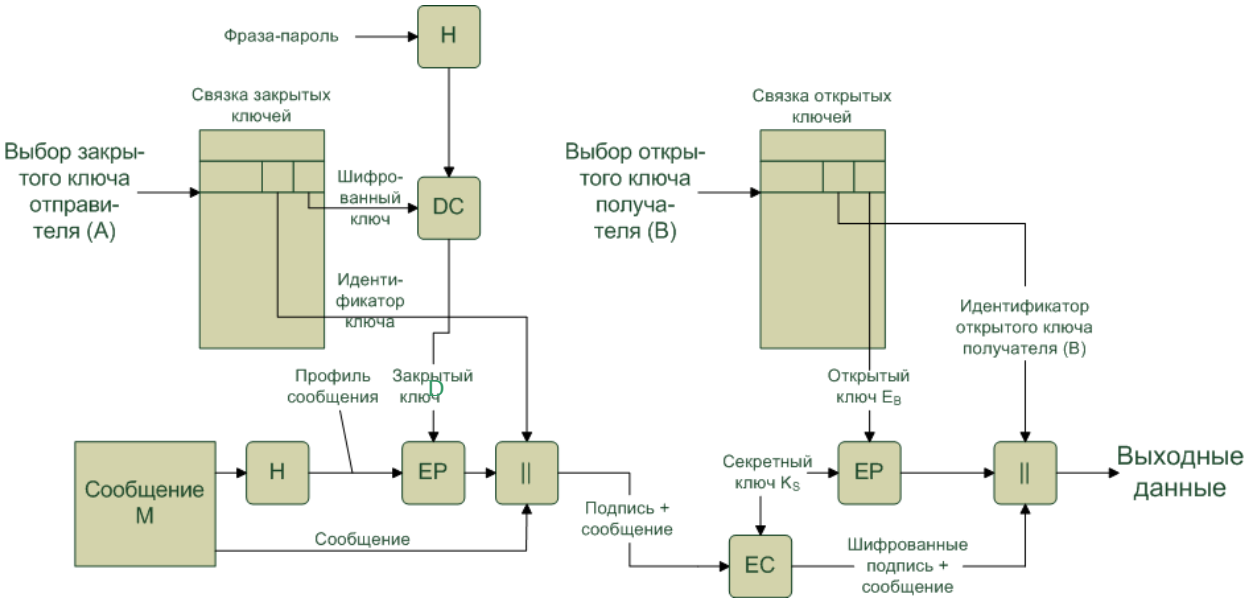


Рис. Е.3. Создание сообщения PGP от А к В

Принимающий объект PGP выполняет следующие шаги (рис. Е.4):

3. Дешифрование сообщения.

- PGP извлекает закрытый ключ получателя D_B из связки закрытых ключей, используя в качестве ключа поиска полученное значение идентификатора открытого ключа получателя (В) $E_B mod 2^{64}$.

- PGP извлекает зашифрованный закрытый ключ получателя В из связки закрытых ключей. Создается хеш-функция фразы пароль, которая служит ключом для того, чтобы с помощью симметричной криптографии DC расшифровать закрытый ключ D_B.

- PGP восстанавливает секретный (общий) ключ Ks ($Ks=D_B[E_B(Ks)]$). С помощью этого

ключа, используя симметричную криптографию DC, дешифрируется сообщение M, профиль этого сообщения (хеш-код) и идентификатор закрытого ключа отправителя $E_a mod 2^{64}$.

4. Аутентификация сообщения.

- PGP извлекает открытый ключ отправителя E_A из связки открытых ключей, используя в качестве ключа поиска поля идентификатор закрытого ключа отправителя.

- PGP вычисляет профиль принятого сообщения M и сравнивает его с расшифрованным профилем, пришедшим вместе с сообщением, чтобы убедиться в их идентичности. При совпадении профилей полученное сообщение считается подлинным.

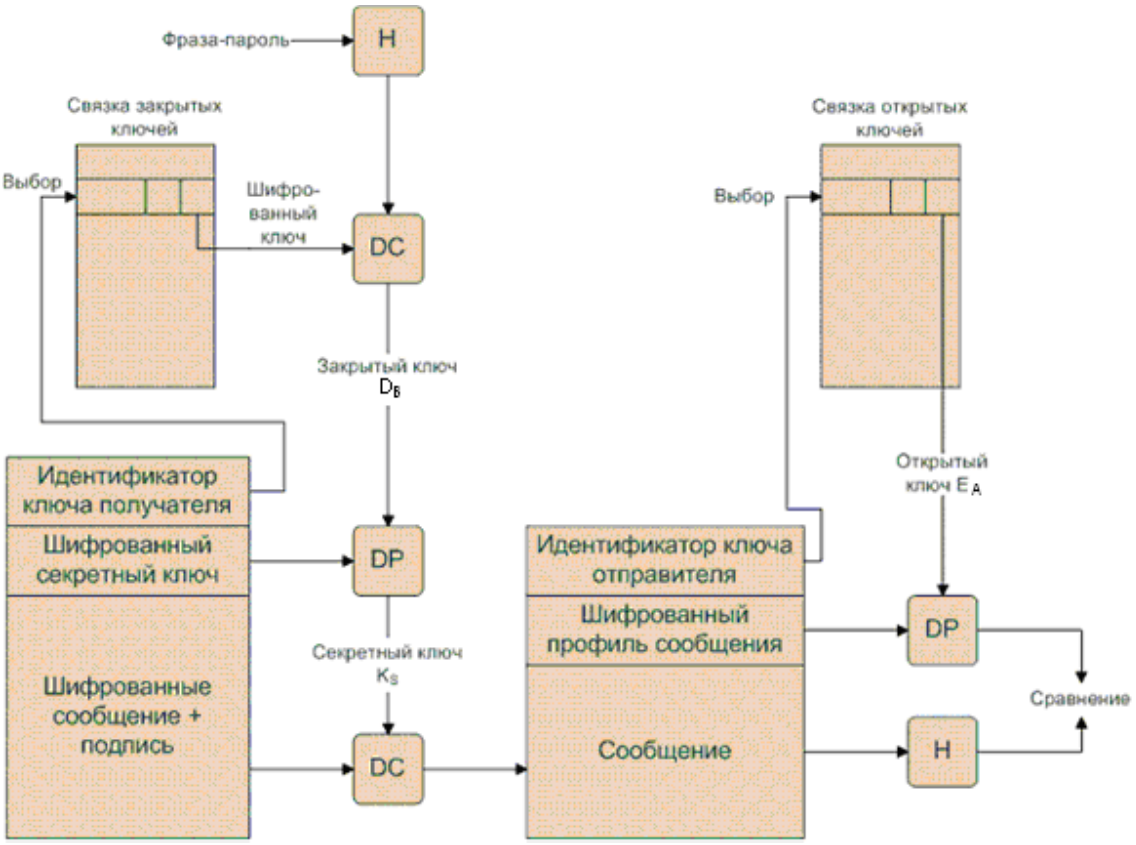


Рис. Е.4. Получение сообщения PGP от А к

ПРИЛОЖЕНИЕ Ж. Протокол ИБ прикладного уровня SET сети TCP/IP

Настоящее приложение посвящено описанию алгоритма протокола ИБ прикладного уровня сети TCP/IP: протокола защищенных электронных транзакций SET (Security Electronic Transaction). Этот протокол используется для защиты информации транзакций, проводимых через Internet, с помощью банковских операций [9].

Протокол электронных платежных транзакций SET является стандартом, принятым основными платежными системами. Текущая версия протокола SET, принадлежащая прикладному уровню сети Internet, появилась ввиду возникшей необходимости создания стандарта защиты для кредитных карт MasterCard и Visa. Под транзакцией здесь понимается использование платежных средств для приобретения товара. Расчеты с использованием пластиковых карт – одна из форм электронных платежей.

Полнофункциональный электронный магазин в общем случае содержит электронную витрину для просмотра и выбора товара, подсистему расчетов с покупателем и службу доставки. Ключевая роль в организации электронного магазина принадлежит подсистеме расчетов, которая взаимодействует с одной или несколькими платежными системами. Кредитные платежные системы – это аналог обычных систем, но только с применением Internet для передачи данных и с обеспечением информационной безопасности. К числу подобных систем относятся Cyber Cash, Check Free, Open Market, First Virtual и другие системы, использующие протокол SET.

Работа системы происходит следующим образом:

1. Покупатель подключается к web-серверу магазина, формирует корзину заказа и отправляет запрос.
2. Магазин в ответ на запрос направляет покупателю счет с электронно-цифровой подписью (ЭЦП).
3. Покупатель подтверждает намерение совершить покупку, для чего подписывает счет уже своей ЭЦП. После подписи покупателем счет становится чеком.
4. Чек с двумя ЭЦП (магазина и покупателя) направляется магазином в банк для авторизации.
5. Банк производит обработку подписанного чека и разрешает (либо не разрешает) проведение платежа.

Ж.1. Требования к протоколу SET

SET является не платежной системой, а набором протоколов защиты и форматов данных, позволяющим защищенным способом использовать существующую инфраструктуру платежных систем пластиковых карточек в открытых сетях типа сети Internet. По сути, SET обеспечивает следующие три вида сервиса ИБ:

- создание защищенного коммуникационного канала, связывающего все участвующие в транзакции стороны;
- обеспечение доверия с помощью цифровых сертификатов;
- обеспечение секретности ввиду того, что информация оказывается доступной только участникам транзакции и только тогда и там, где она необходима.

К протоколу SET предъявляются следующие требования, которые должны соблюдаться при обработке платежей по кредитным картам в Internet:

- конфиденциальность платежа и информации о заказе. Необходимо гарантировать владельцам платежных карт, что данная информация надежно защищена и окажется доступной только тому, кому она предназначена. Под платежной карточкой понимается пластиковая карточка, с помощью которой можно осуществить безналичные платежи. Конфиденциальность к тому же уменьшает риск обмана любой из участвующих в осуществлении транзакции сторон или злоумышленных действий третьей стороны. Для обеспечения конфиденциальности применяется шифрование. Под транзакцией здесь понимается единичный факт использования платежного средства для приобретения товаров, получения наличных или информации по счету, следствием которого является дебетование или кредитование счета клиента. Под дебетованием счета понимается операция списания средств со счета. Под кредитованием понимается операция зачисления средств на счет.
- гарантия целостности передаваемых данных означает, что в ходе передачи информация, содержащаяся в сообщении SET, не претерпит никаких изменений. Для обеспечения целостности служит механизм цифровой подписи;
- аутентификация предъявителя кредитной карточки как законного владельца соответствующего счета. Под кредитной картой понимается денежный документ, предъявляемый клиентом, по которому банки берут на себя риск немедленной оплаты товаров и услуг, приобретаемых их клиентами. Механизм, связывающий предъявителя кредитной карточки с соответствующим номером счета, должен уменьшать вероятность мошенничества и снижать общую стоимость обработки платежей. Для проверки того, что предъявитель кредитной карточки является законным владельцем соответствующего действительно счета, применяются такие средства, как цифровая подпись и сертификаты;

- аутентификация продавца, как лица, имеющего право применять транзакции по кредитным карточкам, с помощью выяснения его связи с соответствующей финансовой организацией. Для этого владельцы платежных карт должны иметь возможность убедиться в подлинности продавцов, которым они могут направить заказные транзакции. В этом случае используются цифровые подписи и сертификаты;
- гарантированное использование лучших конструктивных решений и методов защиты для обеспечения наивысшей степени защиты всех легальных участников электронных коммерческих транзакций.

Основные методы реализации требований к SET

Чтобы соответствовать описанным выше требованиям, в протоколе SET реализованы следующие возможности:

- конфиденциальность информации. Информация о счете владельца карты и платеже защищается во время пересылки по сети. Интересная и важная особенность SET заключается в том, что продавец при этом не может выяснить номер кредитной карточки ее владельца – эта информация оказывается доступной только выдавшему кредитную карточку банку. Для обеспечения конфиденциальности используется шифрование по традиционной схеме с помощью алгоритма DES;
- целостность данных. Информация платежа, посылаемая владельцем карты продавцу, содержит информацию о заказе, личные данные и инструкцию по осуществлению платежа. SET гарантирует, что содержимое этих сообщений не будет изменено на пути их следования. Целостность данных достигается с помощью цифровых подписей RSA, использующих хеш-функцию SHA-1. Некоторые сообщения защищены также с помощью алгоритма HMAC, использующего SHA-1 (Алгоритм аутентификации HMAC подлежит описанию в Приложении Г);
- аутентификация счета владельца карты. SET дает продавцу возможность проверить, является ли предъявитель кредитной карточки законным пользователем соответствующего действительного счета. Для этой цели в SET предусмотрено использование цифровых сертификатов в соответствии со стандартом ITU-T X.509 с подписями с помощью алгоритма с открытым ключом RSA. Длина RSA ключа – 1024 бита;
- аутентификация продавца. SET позволяет владельцу карты проверить, имеет ли продавец отношение к соответствующей финансовой организации и право принимать платежи по кредитным карточкам. Для этой цели в SET предусмотрено использование цифровых сертификатов X.509v3 с подписями RSA.

Участники транзакций SET

На рис. Ж.1 приведены участники транзакций, осуществляемых с помощью SET:

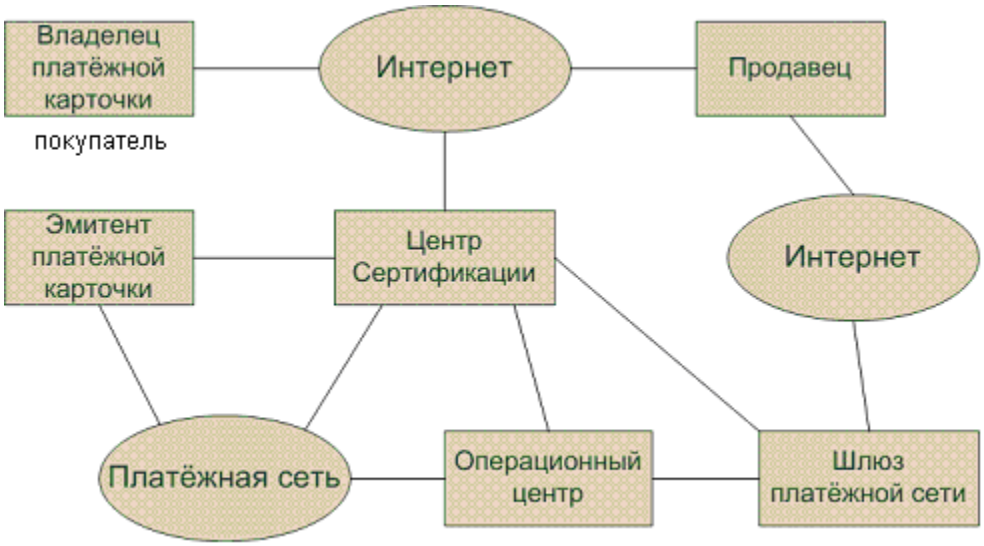


Рис. Ж.1. Участники транзакций SET

- владелец платежной карты. В среде электронных платежей индивидуальные и корпоративные потребители взаимодействуют с продавцами со своих персональных компьютеров через Internet. Владельцем карты в данном случае является любой зарегистрированный владелец пластиковой платежной карты (VISA, MasterCard и т.п.), выданной ему некоторым уполномоченным эмитентом;

- продавец. Продавец является лицом, у которого владелец карты может приобрести товары или услуги. Обычно такие товары или услуги предлагаются на продажу на Web-узле или по электронной почте. Продавец, имеющий право принимать платежи по платежным картам, должен иметь соответствующие отношения с операционным центром;

- эмитент платежной карточки. Финансовая организация (например - банк), выдавшая платежную карточку соответствующему лицу (владельцу карты). Как правило, открыть счет можно по почте или, явившись в офис эмитента, лично. Всю ответственность по оплате задолженности владельца карты по данной карте несет эмитент карты;

- операционный центр (acquirer). Финансовая организация, ведущая расчеты с продавцом, выполняющая авторизацию платежных карт и осуществляющая соответствующие платежи. Продавцы обычно готовы принимать кредитные карты разных видов, но не хотят иметь дело с большим числом разных банковских ассоциаций или множеством отдельных эмитентов платежных карт. Операционный центр проводит для продавца проверку того, что счет кредитной карты является действительным, и предлагаемая покупка по стоимости не

выходит за рамки допустимого кредитного лимита. Операционный центр также выполняет электронный перевод денежных сумм на счет продавца. Впоследствии операционный центр получает за это определенную компенсацию от эмитента карты через банковскую платежную сеть;

- шлюз платежной сети (payment gateway). Совокупность средств, контролируемых операционным центром или уполномоченной им третьей стороной и используемых для обработки платежных сообщений продавца. Шлюз платежной сети связывает SET и существующие банковские платежные сети, выполняя функции авторизации и передачи платежей. Продавец обменивается сообщениями SET с шлюзом платежной сети через Internet, а шлюз платежной сети связан непосредственно или по внутренней сети с системой обработки финансовых документов соответствующего операционного центра;

- центр сертификации ЦС. Объект, которому доверяется право выдавать сертификаты открытых ключей владельцев карт, продавцов и шлюзов платежной сети. Успешная работа SET во многом зависит от наличия хорошо организованной инфраструктуры сертификации, доступной для использования в соответствующих целях. Как уже говорилось в главе 5, обычно используется иерархия центров сертификации, так что участники системы электронных платежей могут быть сертифицированы не только главным центром сертификации непосредственно.

Опишем последовательность событий, происходящих во время транзакции, а затем остановимся подробнее на некоторых криптографических деталях данного процесса:

- *покупатель открывает счет*. Покупатель открывает счет кредитной карточки (например, VISA или MasterCard) в банке, осуществляющем электронные платежи и поддерживающем SET;

- *покупатель получает сертификат*. После установленной процедуры проверки личности покупатель получает цифровой сертификат, подписанный банком. Этот сертификат удостоверяет открытый ключ RSA покупателя и срок действия этого ключа. Он также устанавливает гарантированное банком соответствие между парой ключей покупателя и его кредитной карточкой;

- *продавец получает свои сертификаты*. Продавец, который собирается принимать оплату по платежной карточке определенного типа, должен получить два сертификата двух своих открытых ключей: один из них будет использоваться для цифровой подписи, а второй – для обмена ключами. Продавцу потребуется копия сертификата открытого ключа шлюза платежной сети;

- *покупатель размещает заказ*. Этот процесс может предполагать, что покупатель сначала

должен посетить Web-узел продавца, чтобы выбрать подходящий товар и определить цену. После этого покупатель отправляет продавцу список нужных ему товаров, а продавец в ответ высылает бланк заказа с указанными в нем списком выбранных товаров, ценами, общей стоимостью заказа и номером заказа;

- *проверка продавца*. Вместе с бланком заказа продавец высылает копию своего сертификата, чтобы покупатель имел возможность убедиться в том, что он действительно имеет дело с настоящим продавцом;

- *заказ и платеж отправляются продавцу*. Покупатель отправляет заказ и платежную информацию продавцу, прилагая к ним свой сертификат. Заказ подтверждает покупку товаров, указанных в бланке заказа. Платёжная информация содержит необходимые данные заказа. Платежная информация шифруется таким образом, чтобы продавец не смог ее прочесть. Сертификат покупателя позволяет продавцу выполнить проверку покупателя;

- *продавец запрашивает авторизацию платежа*. Продавец отправляет платежную информацию шлюзу платежной сети с запросом подтверждения того, что доступный покупателю кредит достаточен для осуществления данного платежа. В ответ продавец получает разрешение на оплату;

- *продавец подтверждает заказ*. Продавец отправляет покупателю подтверждение заказа;

- *продавец доставляет товары или предоставляет услуги*. Продавец организует доставку товаров или выполнение услуг покупателю;

- *продавец запрашивает получение платежа*. Этот запрос отправляется шлюзу платежной сети, который обрабатывает все платежные поручения.

Ж.2. Дуальная подпись

Прежде чем перейти к рассмотрению деталей протокола SET, приведем описание процедуры, так называемой дуальной (двойной) подписи DS (dual signature), применяемой в SET.

Дуальная подпись позволяет связать два сообщения, предназначенные двум разным получателям. В данном конкретном случае покупателю требуется переслать информацию о заказе (Order Information - OI) продавцу и платежную информацию (Payment Information – PI) банку. Продавцу не нужно знать номер кредитной карточки покупателя, а банку не нужны подробности заказа. Покупатель же, разделяя эти сведения, обеспечивает тем самым дополнительную защиту своих прав с точки зрения невмешательства в его личные данные. При этом требуется связать эти сведения так, чтобы их можно было использовать при возникновении конфликта. Связь разделенных сведений требуется для того, чтобы

покупатель мог доказать, что данный платеж предназначен для оплаты именно этого, а не какого-то другого заказа.

Чтобы понять необходимость такой связи, предположим, что покупатель отправляет продавцу два подписанных сообщения - OI (заказ) и PI (платеж), а продавец пересылает сообщение PI в банк. Если продавец получит от покупателя какой-то другой заказ, то продавец сможет заявить, что данное сообщение PI оплачивает новое, а не старое сообщение OI. Связывание исключает такую возможность.

На рис. Ж.2 показана схема использования дуальной подписи для решения сформулированной проблемы. Сначала покупатель, используя алгоритм SHA-1, вычисляет хеш-коды для сообщений PI и OI. Два полученных хеш-кода связываются операцией конкатенации, и для результата связывания тоже вычисляется хеш-код. Наконец, покупатель шифрует итоговый хеш-код с использованием своего закрытого ключа цифровой подписи, в результате получая дуальную подпись.

Вся процедура формально может быть записана в следующем виде:

$$D = D_n \left[H\left(H_d(P) \| H(O) \right) \right] = D_n \left[H(P_o I \mid O_к \mid) \right] = D_n \left[PMI_o \right], \qquad (1)$$

где $D_{пок}$ - закрытый ключ цифровой подписи покупателя;

H - функция хеширования;

PIMD – профиль сообщения PI,

OIMD – профиль сообщения OI.

Теперь предположим, что продавец имеет дуальную подпись DS, сообщение OI и профиль сообщения PI (PIMD). Кроме того, у продавца есть открытый ключ покупателя $E_{пок}$. В таких условиях продавец может вычислить два следующих значения:

$$P = H\left(H(P) \| H(O) \right) = H\left(H(PM) \| O \right) \qquad (2)$$

$$P' = E_n \left[D_o \right] \qquad (3)$$

где $E_{пок}$ – открытый ключ цифровой подписи покупателя.

Если оба значения оказываются равными (POMD' = POMD), то продавец считает, что подпись проверена. Точно так же, имея DS, PI, профиль сообщения OI (OIMD) и открытый ключ покупателя, банк может вычислить H(H(PI)||OIMD) и $E_{пок}$ [DS].

Если эти значения оказываются равными, банк считает, что подпись покупателя проверена.

Предположим, что продавец решит заменить сообщение OI данной транзакции другим, с целью извлечь из этого выгоду. Для этого ему придётся найти другое сообщение OI с точно таким же хеш-кодом OIMD. Как было показано выше, для алгоритма SHA – 1 с длиной хеш-

кода 160 бит такая задача злоумышленника неразрешима практически. Таким образом, у продавца нет возможности связать с данным сообщением PI другое сообщение OI.

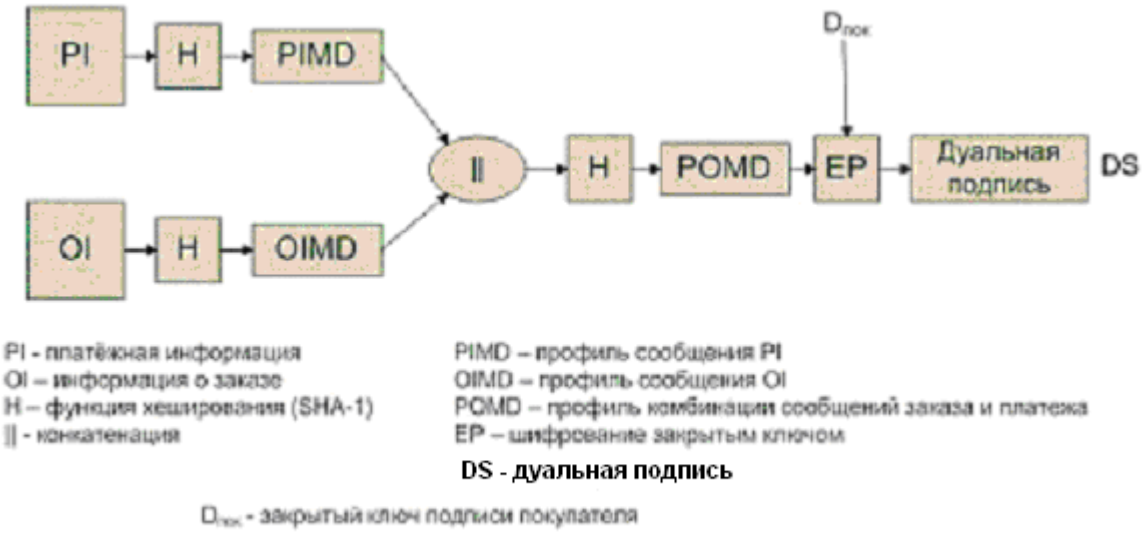


Рис. Ж.2. Создание дуальной подписи

Подводя итог, можно сказать следующее:

- продавец получает сообщение OI и выполняет проверку подписи покупателя;
- банк получает сообщение PI и выполняет проверку подписи покупателя
- сообщения OI и PI оказываются связанными, и покупатель может доказать их связь.

Ж.3. Обработка платежей

В таблице Ж.1. перечислены некоторые из типов транзакций, поддерживаемых SET. В работе [9] приведен список 14 типов транзакций. В данном разделе рассмотрению подлежат следующие три типа транзакций

- требование на закупку (Purchase Request);
- разрешение на оплату (Payment Authorization);
- получение оплаты (Payment Capture)

Таблица Ж.1. Некоторые типа транзакций SET

Название	Описание
Cardholder registration	Владельцы платежных карт должны зарегистрироваться в

(регистрация владельца карты)	центре сертификации, для возможности отправлять сообщения SET продавцам
Merchant registration (регистрация продавца)	Продавцы должны зарегистрироваться в центре сертификации, чтобы иметь возможность обмениваться сообщениями SET с покупателями и шлюзами платежной сети
Purchase request (требование на закупку)	Сообщение, отправляемое покупателем продавцу, содержащее OI для продавца и PI для банка
Payment authorization (разрешение на оплату)	Последовательность сообщений, которыми обмениваются продавец с шлюзом платежной сети для авторизации соответствующего платежа со счета соответствующей кредитной карточки
Payment capture (получение оплаты)	Позволяет продавцу запросить получение соответствующего платежа у шлюза платежной сети
Certificate inquiry and status (запрос сертификата и его статуса)	Если центр сертификации не может быстро обработать адрес на получение сертификата, в ответ покупателю или продавцу отправляется сообщение о том, что запрашивающей стороне нужно обратиться за ответом на запрос повторно позже. Владелец платежной карточки или покупатель посылает сообщение Certificate Inquiry для того, чтобы выяснить состояние процесса обработки его запроса сертификата и получить сертификат, если запрос был удовлетворен

На рис. Ж.3 приведены: диаграмма обмена сообщениями обработки транзакции «Требование на закупку», «Разрешение на оплату», «Получение оплаты»; состав этих сообщений; принятые обозначения. Процедура обработки транзакции «Требование на закупку» выполняется в результате обмена сообщениями 1-10, транзакции «Разрешение на оплату» - сообщениями 11 - 14, транзакции «Получение оплаты» - сообщениями 15 -17. На диаграмме приведена запись каждого из этих сообщений в принятых для этой цели обозначениях. Описание обработки каждой из этих транзакций приводится в следующих подразделах.

1. $(И\ ) - (ЗИ\quad ЗИ\ 1\ R3)$
2. $(О\quad) - И\quad , R1, ИR2, D_п\ [H(И_р\quad ЗR1, ЗR2)], «ПТ\ », «Шл'»$
3. Дайте сертификат «Пр» продавца для цифровой подписи
4. Получите сертификат «Пр» для цифровой подписи
5. Дайте сертификат «Шл'» для цифрового конверта (обмена ключами)
6. Получите сертификат «Шл'» для цифрового конверта (обмена ключами)
7. $(Т\ ) - (О\ , D\ , Р\quad), «П\ », K_s[Р\ , D\ , О\quad], E'_ш\ [K_s], R2$
8. $(О\quad) - (Б\quad , И\quad), D_п\ (H(ПБ\ \ О, И_р\quad))), «ПП\ »$
9. Дайте сертификат для цифровой подписи продавца «Пр»
10. Получите сертификат для цифровой подписи продавца «Пр»
11. ,$E'_{шл}$ [K_s]
12. Запрос разрешения на оплату
13. Разрешение на оплату
14. $(О\quad - И\ ) - K_{S2}[Б\ , DЗ_ш\ (H(БА))], E'_п\ (K_{s2}), «ШПА»$
    $(О\quad - И\quad) - K_{S2}[Б\ ЗD_ш\ (HИ(Б\ ))\quad РА_п$
15. $(З\quad) - K_{S2}O[Б\quad , D_п\ (H(Б\quad))]OE'_шЗ\ (K_{S3}), «ОП\ », «Пр'»$
    $(З\quad - И\ О) - K_{S2}[ИБ\ , D_ш\ (HА(БД))]\qquad A$
16. Расчетный запрос
17. $(О\quad) - K_{S4}[БЗ\quad , D_ш\ (ОН(Б_л\quad))], E'_пЗО(K_{S4}), «ШОл'»$

Принятые обозначения

«Пр», $E_{пр}$, $D_{пр}$ – сертификат, открытый ключ, закрытый ключ продавца для цифровой подписи;

«Пр'», $E'_{пр}$, $D'_{пр}$ – сертификат, открытый ключ, закрытый ключ продавца для обмена

одноразовыми симметричными ключами;

«Шл», $E_{шл}$, $D_{шл}$ – сертификат, открытый ключ, закрытый ключ шлюза платежной сети для цифровой подписи;

«Шл'», $E'_{шл}$, $D'_{шл}$ – сертификат, открытый ключ, закрытый ключ шлюза платежной сети для обмена одноразовыми симметричными ключами;

«Пок», $E_{пок}$, $D_{пок}$ – сертификат, открытый ключ, закрытый ключ покупателя для дуальной подписи.

Рис. Ж.3. Диаграмма обмена сообщениями обработки транзакций

Ж.3.1. Обработка транзакции «Требование на закупку»

До того как начать обмен данными требования на закупку (Purchase Request), владелец платежной карточки должен завершить просмотр списка доступных товаров, выбрать нужные и оформить заказ. Данный предварительный этап заканчивается отправкой продавцом бланка заказа покупателю. Все эти предварительные операции не связаны с SET.

Обмен данными требования на закупку состоит из сообщений: Initiate Request (инициирующий запрос), Initiate Response (ответ на инициирующий запрос), Purchase Request (требование на закупку) и Purchase Response (ответ на требование на закупку).

В сообщение 1, рис. Ж.2 (ИЗ – инициирующий запрос) входят:

- информация о типе кредитной карты, используемой покупателем (ИЗ1);
- запрос на получение сертификатов продавца и шлюза (ИЗ2);
- случайное число, сгенерированное оборудованием покупателя и предназначенное для защиты от угрозы «повтор» (R1).

Сообщение 1 не подлежит шифрованию и отправляется без цифровой подписи.

Продавец отправляет «Ответ на инициирующий запрос» ОИЗ (сообщение 2). В ОИЗ входят:

- случайное число R1 для подтверждения того, что оно было отправлено им в предыдущем сообщении 1;
- случайное число, сгенерированное оборудованием продавца и предназначенное для защиты от угрозы «повтор» (R2);
- идентификатор (данной) транзакции (ИТР);
- сертификат для цифровой подписи продавца («Пр»). В SET предусмотрено две пары (открытый, закрытый) ключей продавца. Одна из них предусмотрена для

цифровой подписи сообщения, а другая для обмена одноразовыми ключами симметричного шифрования.

- сертификат шлюза платежной системы («Шл'») для обмена одноразовыми ключами симметричного шифрования. Предполагается наличие двух пар ключей шлюза платёжной сети (одной для цифровой подписи, другой – для обмена одноразовыми ключами симметричного шифрования).

На схеме не приводится путь получения этого сертификата (от шлюза через продавца).

В сообщение 2 входит также электронно-цифровая подпись (ЭЦП) всей информации ответа на инициирующий запрос, кроме сертификатов, т.е. $D_{пр}[H(ИТР, R1, R2)]$, где $D_{пр}$ – закрытый ключ для цифровой подписи продавца, H(ИТР, R1, R2) – хеш-функция сообщения. Покупатель (владелец платежной карточки) проверяет подлинность открытых ключей сертификатов продавца и шлюза платежной сети. На диаграмме рис. Ж.3 приведены запросы (сообщения 3 и 5) на получения сертификатов продавца и шлюза и соответствующие ответы (сообщения 4 и 6). Подробное описание проверки правильности открытого ключа с помощью сертификатов приведено в приложении В.

В случае положительного результата проверки сертификатов покупатель проверяет ЭЦП, полученную в сообщении 2. Проверка проводится с помощью открытого ключа продавца $E_{пр}$, в правильности которого мы убедились в результате проверок сертификатов. Подробное описание проверки ЭЦП сообщения приведено выше в приложении В.

Теперь покупатель формирует сообщение 7 требование на закупку ТЗ (рис. Ж.4). В это сообщение входит информация о заказе OI. Эта информация представляет собой данные о заказе. Они является открытыми для покупателя и продавца и формируются на этапе согласования между ними еще до отправки сообщения «инициирующий запрос» (сообщение 1). В сообщение 7 включен PIMD – профиль сообщения платежной информации PI, который предназначен для передачи в шлюз платежной системы. В PI содержится номер кредитной карточки покупателя (которую не должен знать продавец), а также идентификатор транзакции ИТР. Таким образом, в сообщении 7 содержится информация, предназначенная двум разным сторонам (продавцу и шлюзу платежной сети). Как было отмечено выше, дуальная подпись позволяет связать два сообщения, т.е. PI и OI. В оба эти сообщения помещается идентификатор транзакции ИТР, сформированный продавцом в сообщении 2. Для того чтобы информация PI не была прочитана продавцом, покупатель отправляет ее в зашифрованном виде с помощью сгенерированного им одноразового секретного ключа симметричного шифрования K_s. В сообщение 7 (требование на закупку) входят (рис. Ж.3):

- информация о платеже $K_s[PI, DS, OIMD]$, $E'_{шл}(K_s)$,R2;

- информация о заказе OI, DS, PIMD;
- сертификат владельца платежной карточки «Пок», т.е. покупателя.

Зашифрованная информация о платеже пересылается продавцом шлюзу платежной сети и содержит следующие данные:

- данные PI;
- дуальная подпись DS, вычисленная для совокупности PI и OI и подписанная с использованием закрытого ключа подписи покупателя;
- профиль сообщения OI (OIMD). Значение OIMD необходимо для того, чтобы шлюз платежной сети мог проверить дуальную подпись, как объяснялось выше. PI, DS и OIMD шифруются с помощью ключа K_s;
- цифровой конверт ($E'_{шл}$ [K_s]) формируется путем шифрования Ks с помощью открытого ключа шлюза платежной сети, $E'_{шл}$, предназначенного для обмена ключами. Этот элемент называется цифровым конвертом, поскольку для того, чтобы получить возможность прочитать элементы, перечисленные выше, этот конверт необходимо открыть (т.е. расшифровать) закрытым ключом шлюза $D'_{шл}$.

Значение K_s остается продавцу неизвестным. Поэтому продавец не сможет прочитать ничего из всей относящейся к этому платежу информации.

Информация о заказе требуется продавцу и содержит следующие данные:

- данные OI;
- дуальная подпись DS, вычисленная для совокупности PI и OI и подписанная с использованием закрытого ключа подписи покупателя;
- профиль сообщения PI(PIMD).

Значение PIMD необходимо для того, чтобы продавец мог проверить правильность дуальной подписи DS, как показано и проиллюстрировано в разделе Ж.2. Заметим, что данные OI отправляются в открытом виде.

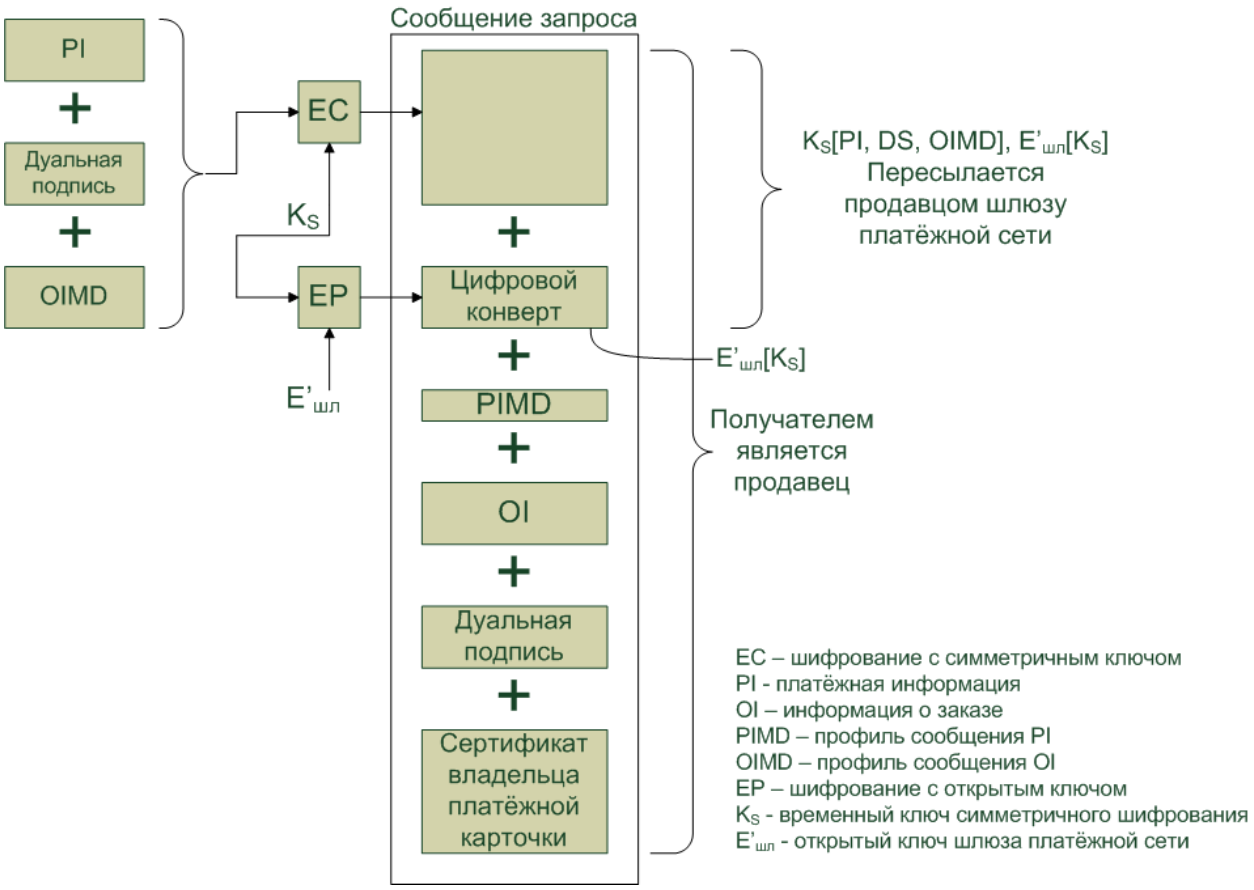


Рис. Ж.4. Структура сообщения «Требование на закупку» (ТЗ)

Сертификат владельца платежной карточки покупателя «Пок» содержит открытый ключ покупателя. Этот сертификат необходим как продавцу, так и шлюзу платежной сети для дуальной подписи.

После получения сообщения 7 продавец выполняет следующие действия:

- проверяет сертификаты владельца платежной карточки с помощью содержащихся в них подписей центров сертификации (на диаграмме рис. Ж.3 не показано);
- проверяет (как описано в разделе Ж.2 и проиллюстрировано на рис. Ж.5) дуальную подпись с помощью открытого ключа цифровой подписи владельца платежной карточки $E_{пок}$. Это позволяет убедиться в том, что заказ не был изменён во время пересылки и был подписан владельцем платёжной карточки;
- обрабатывает заказ и пересылает платежную информацию шлюзу платежной сети для платежа (соответствующий процесс будет описан ниже);
- отправляет сообщение 8 ОТЗ (ответ требованию на закупку) владельцу

платежной карточки.

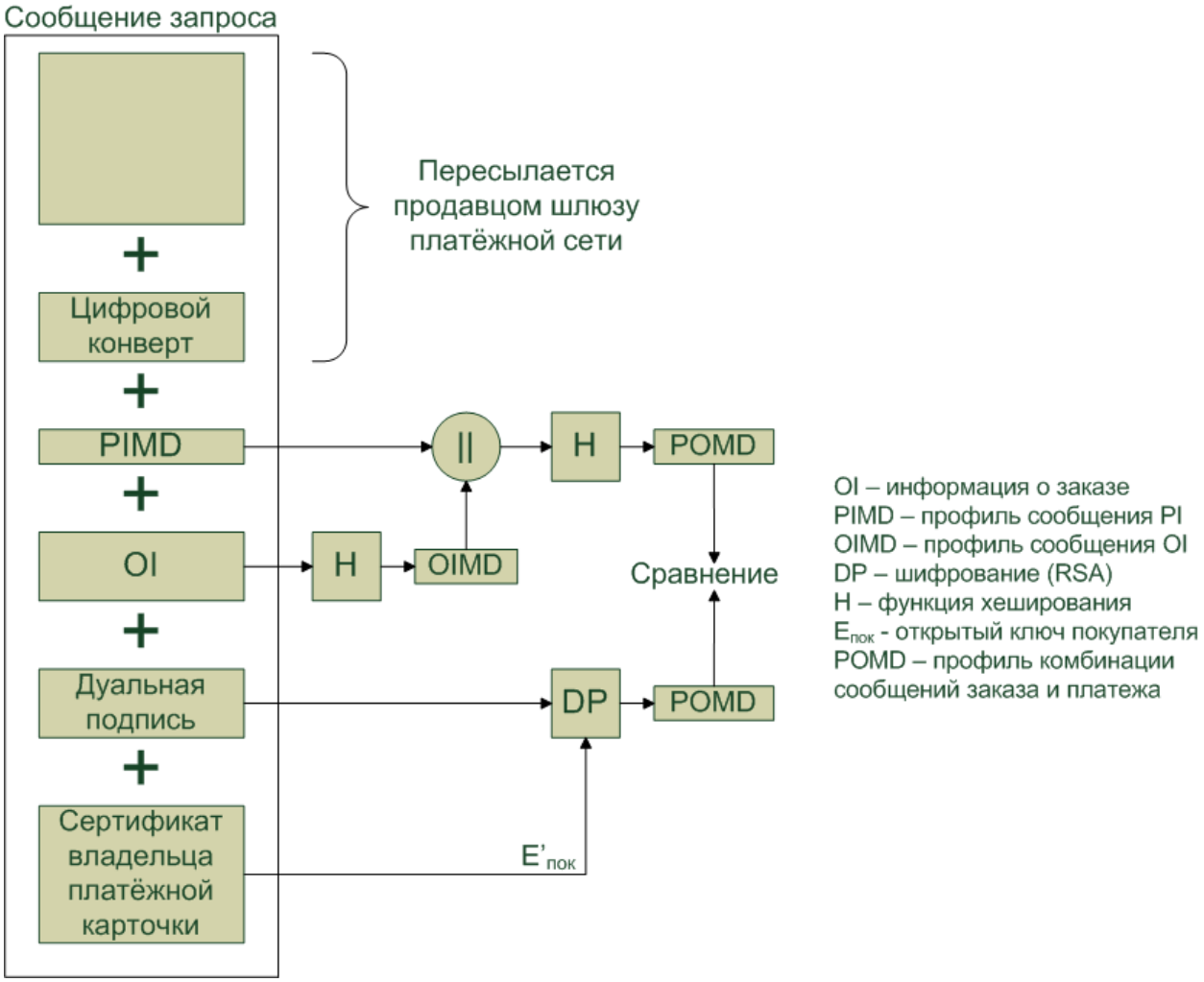


Рис. Ж.5. Обработка сообщения «Требование на закупку» продавцом

Сообщение 8 содержит БО (блок ответа), подтверждающий заказ и идентификатор транзакции (ИТР). В сообщении 8 содержится также сертификат продавца «Пр». Все данные, входящие в ОТЗ, кроме «Пр», подписываются продавцом с помощью его закрытого ключа $D_{пр}$.

Когда покупатель получает сертификат продавца, производится снова проверка его подлинности (сообщения 9 и 10), как это было при получении сообщения 2. Убедившись в подлинности сертификата, а значит и входящего в него открытого ключа продавца, проверяются остальные данные сообщения 8 с помощью ЭЦП. При положительном результате выполняются соответствующие действия, например, отображение на экране некоторых сообщений для покупателя или обновляется информация в состоянии заказа в базе данных.

Ж.3.2. Обработка транзакции «Разрешение на оплату»

Процедура обработки транзакции «Разрешение на оплату» выполняется в результате обмена сообщениями 11-14 диаграммы рис. Ж.3.

Во время обработки сообщения 7 (ТЗ - требование на закупку) продавец одновременно с отправкой сообщения 8 покупателю, как было отмечено выше, обрабатывает заказ и пересылает зашифрованную платежную информацию (PI) шлюзу платежной сети для авторизации платежа (получение разрешения на оплату). Такое получение разрешения на оплату означает санкционирование транзакции эмитентом платежной карточки. Авторизация дает продавцу гарантию того, что он получит плату за проданный товар, и поэтому продавец может выполнить доставку товаров покупателю. Обмен данными для получения разрешения па оплату формируется из двух сообщений: Authorization Request (запрос разрешения на оплату ЗРО - сообщение 11) и Authorization Response (ответ на запрос разрешения на оплату ОЗР - сообщение 13).

Сообщение 11 (ЗРО - запрос разрешения на оплату), отправляемое продавцом шлюзу платежной сети, состоит из следующих блоков информации:

- информация о платеже, полученная от покупателя и содержащая данные P1 в составе сообщения 7 – K_s(P1, DS, OIMD) и цифровой конверт $E'_{шл}[K_s]$;
- информация авторизации;
- сертификаты.

Информация авторизации генерируется продавцом и содержит следующие данные:

- блок авторизации (БА), включающий идентификатор транзакции ИТР и другие значения. БА подписан закрытым ключом продавца $D_{пр}$. БА и подпись шифруются генерируемым продавцом одноразовым ключом симметричного шифрования K_{s1} - K_{s1}[БА, $D_{пр}$(H(БА))];
- цифровой конверт, сформированный шифрованием одноразового секретного ключа K_{s1}, с помощью открытого ключа шлюза платежной сети – $E'_{шл}(K_{s1})$. Цифровой конверт предназначен для обмена ключами.

В сообщение 11 входят следующие сертификаты:

- сертификат владельца платежной карточки «Пок», который служит для проверки дуальной подписи;
- сертификат продавца «Пр», который служит для проверки цифровой подписи продавца;

- сертификат продавца «Пр'», который служит для обмена секретными ключами.

Обратим внимание на то, что продавец получает два сертификата для общения со шлюзом платежной сети. Сертификат цифровой подписи продавца «Пр» с открытым ключом для проверки цифровой подписи продавца в сообщениях, отправленных в шлюз (ключ $E_{пр}$). Сертификат «Пр'» для формирования цифрового конверта, содержащего секретный ключ симметричного шифрования и направляемого в шлюз. Шлюз платежной сети проверяет подлинность обоих сертификатов продавца и сертификата покупателя. На диаграмме рис. Ж.3 обмен этими сообщениями между шлюзом и центром сертификации не показан. Получив сообщение 11, шлюз платежной сети выполняет следующие действия:

- расшифровывает цифровой конверт $E'_{шл}(K_{s1})$ с помощью закрытого ключа шлюза, т.е.

$$K_{s1} = D'_{ш}\left(E'_{ш}\left(K_{s1}\right)\right) \quad (4)$$

где K_{s1} – одноразовый ключ симметричного шифрования продавца;

$D'_{шл}$ – закрытый ключ шлюза платежной сети;

$E'_{шл}$ – открытый ключ шлюза платежной сети;

– расшифровывает блок авторизации (БА)

$$БА, D_{пр}(H(БА) = Ks_1\{Ks_1[БА, D_{пр}(H(БА))]\} \quad (5)$$

- проверяет подпись продавца для блока данных авторизации БА с помощью открытого ключа продавца $E_{пр}$;

– расшифровывает цифровой конверт блока платежной информации, т.е.

$$K_s = D'_{ш}\left(E'_{ш\,л}(K_s)_n\right) \quad (6)$$

где K_s – одноразовый ключ симметричного) шифрования, покупателя.

расшифровывает блок платежной информации, т.е.

$$K_s\left(K_s\left(P\ ,D\ ,C\right)\right) = P\ ,D M,C \quad (7)$$

- проверяет дуальную подпись блока платежной информации (как описано в разделе Ж.2 и проиллюстрировано на рис. Ж.6)

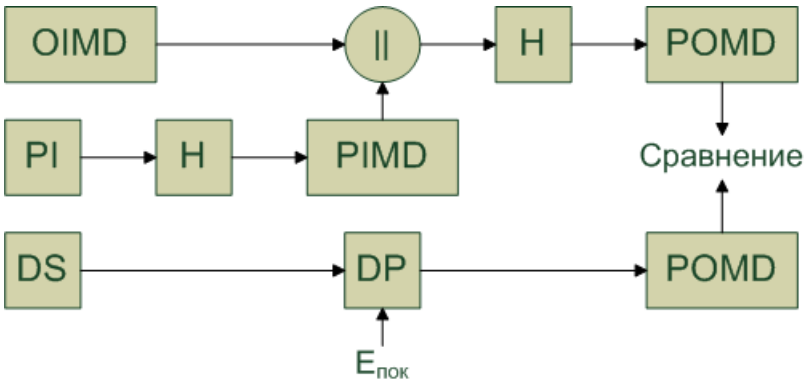


Рис. Ж.6. Проверка дуальной подписи в шлюзе платежной сети

- проверяет совпадение идентификатора транзакции (ИТР), полученного or продавца в БА, с идентификатором транзакции ИТР, включенным в состав данных PI и поступившего от владельца платежной квитанции (через продавца);
- при положительном результате сравнения запрашивает и получает разрешение на оплату у эмитента платежной карточки (банка покупателя) сообщениями соответственно 12 и 13.

Получив разрешение на оплату у эмитента платежной карточки, платежный шлюз возвращает продавцу сообщение ОЗР (ответ запроса разрешения на оплату - Authorization Response) – сообщение 14. Это сообщение состоит из следующих блоков информации:

- информация авторизации (ИА). На рис. Ж.3 этот блок ОЗР обозначен ОЗР-ИА. Включает блок авторизации БА (идентификатор транзакции ИТР и другие значения). БА был передан в шлюз платежной сети в сообщении 11. Блок авторизации шифруется секретным ключом K_{s2} сгенерированным шлюзом платежной сети – K_{s2}(БА). Этот ключ передается в цифровом конверте, зашифрованный открытым ключом продавца $E'_{пр}$, т.е. $E'_{пр}(K_{s2})$. Зашифрованный БА передается вместе с ЭЦП – $D_{шл}$(Н(БА)). БА и ЭЦП этого блока шифруется ключом K_{s2}, т.е. K_{s2}[(БА), $D_{шл}$(Н(БА))];
- информация манданта на получение платежа ИМП (capture token). На рис. Ж.3 этот блок ОЗР обозначен ОЗР-ИМП. Эта информация будет использована позже для осуществления платежа. Данный блок содержит все те же данные, что и предыдущая информация авторизации. Блок ОЗР-ИМП, в отличие от ОЗР-ИА, не обрабатывается продавцом, а должен быть возвращен в том же виде шлюзу платежной сети;
- сертификат. Сертификат шлюза платежной сети «Шл». Открытый ключ этого сертификата предназначен для обработки транзакции «Получение оплаты». В отличие

от сертификата шлюза «Шл'» в сообщении 2 открытый ключ сертификата «Шл» в сообщении 13 предназначен для ЭЦП, а не для передачи секретного ключа симметричного шифрования.

Получив сообщение 14, продавец определяет блок авторизации БА и его ЭЦП, расшифровав секретным ключом K_{s2}. Ключ K_{s2} определяется из цифрового конверта с помощью закрытого ключа продавца $D'_{пр}$, т.е.

$$K_{s2} = D'_n\left(E'_{pn}\left(K_{s2}\right)\right) \qquad (8)$$

где $D'_{пр}$ – закрытый ключ продавца для обмена ключами;

$E'_{пр}$ – открытый ключ продавца для обмена ключами;

K_{s2} – ключ симметричного шифрования, генерируемый продавцом.

В результате получаем БА, т.е.

$$Б\ , D_ш\left(H(Б\ )\right) = K_{s2}\left[K_{s2}\left(Б_л\right), D_ш\left(H(Б\ )\right)\right] \qquad (9)$$

Используя открытый ключ цифровой подписи шлюза $E_{шл}$, продавец убеждается в подлинности и целостности БА, составной частью которого является идентификатор транзакции ИТР.

Отметим, что открытый ключ сертификата шлюза «Шл» предварительно подлежит такой же проверке, как и сертификат «Шл'» при приеме сообщения 2. На диаграмме рис. Ж.3 обмен сообщениями между шлюзом и центром сертификации не приведен. Совпадение полученного ИТР с тем, который есть у продавца, подтверждает авторизацию платежа от шлюза платежной сети. Продавец теперь может выполнить доставку товаров или услуг покупателю и перейти к обработке транзакции «Получение оплаты».

Ж.3.3. Обработка транзакции «Получение оплаты»

Процедура обработки транзакции «Получение оплаты» выполняется в результате обмена сообщениями 15-17 диаграммы рис. Ж.3.

Для получения оплаты продавец отправляет в шлюз платежной сети сообщение 15 «Запрос на оплату» (ЗО). В это сообщение входит блок данных запроса на оплату (БЗО), включающий сумму платежа и идентификатор транзакции ИТР.

БЗО вместе с подписью шифруется генерируемым продавцом одноразовым секретным ключом K_{s3} – K_{s3}[БЗО, $D_{пр}$(Н(БЗО))]. В состав сообщения 15 входит цифровой конверт $E'_{шл}$ (K_{s3}). Данное сообщение включает также полученный ранее в сообщении 14 мандант на получение платежа ОЗР-ИМП для данной транзакции. Этот мандант на рис. Ж.3 в сообщении 15 обозначен ЗО-ИМП. В шлюз направляются также сертификаты ключей продавца для цифровой подписи и обмена секретными ключами («Пр», «Пр'»).

Получив это сообщение, шлюз платежной сети выполняет следующие действия:

- проверяет полученные сертификаты в результате обмена сообщениями между шлюзом и центром сертификации;
- расшифровывает цифровой конверт $E'_{шл}(K_{s3})$ с помощью закрытого ключа шлюза, т.е.

$$K_{s3} = D'_{ш}\left(E'_{лш}\left(K_{лs3}\right)\right) \qquad (10)$$

где K_{s3} – одноразовый ключ симметричного шифрования, продавца.

Дешифрирует БЗО с ЭЦП, т.е.

$$Б\quad, D_n\left(H(Б\quad)\right) = \overline{p}\, K_{s3}\left[K_{s3}\left(Б\quad, D_n\left(H(Б\quad)\right)\right)\right] \qquad (11)$$

проверяет ЭЦП блока БЗО с помощью открытого ключа продавца $E_{пр}$;

- продавец проверяет информацию мандата на получение платежа, принятого продавцом ОЗР-ИМП в сообщение 14 и возвращенного ЗО-ИМП обратно в сообщении 15.

При известных секретном ключе K_{s2} и открытом ключе шлюза $E_{шл}$ шлюз расшифровывает и проверяет ЭЦП блока авторизации. Так как в блок авторизации БА и в блок запроса на оплату БЗО входит идентификатор транзакции ИТР, то проверяется их совпадение.

При совпадении шлюз платежной отсылает расчетный запрос (сообщение 16) эмитенту платежной карточки по закрытой платежной сети. В результате этого запроса средства перечисляются на счет продавца. Затем шлюз платежной сети в сообщении 17 ОЗО (ответ на запрос оплаты) извещает продавца о перечислении средств. Сообщение 17 содержит блок данных ответа на запрос на оплату (БОЗО). БОЗО шифруется секретным ключом K_{s4} вместе с ЭЦП этого блока. Ключ K_{s4} передается в цифровом конверте, зашифрованным открытым ключом продавца $E'_{пр}(K_{s4})$. ЭЦП блока БОЗО формируется с помощью закрытого ключа шлюза – $D_{шл}(H(БОЗО))$. Кроме этого сообщение 17 содержит сертификат шлюза для цифровой подписи «Шл'».

Алгоритм обработки принятого сообщения 17 аналогичен обработке сообщения ОЗР (сообщение 14).

Контрольные вопросы

1) Какие основные отличия ЕСЭ России по сравнению со многими развитыми странами мира?

а) меньший уровень телефонизации и развития современных технологий

б) большое количество устаревшей аналоговой техники на сетях

в) ограниченность ресурсов радиочастотного спектра

2) К какой категории сети связи относится сеть оператора «Ростелеком»?

а) выделенная сеть связи

б) сеть связи общего пользования

в) технологическая сеть связи

г) сеть специального назначения.

3) Какая технология распределения информации принята стратегическим направлением новой техники связи (в соответствии с законом «О связи»)?

а) коммутация каналов

б) коммутация пакетов

в) коммутация сообщений

г) коммутация пакетов и коммутация сообщений

4) Какой вид услуг в Единой сети связи России относится к универсальной (в соответствии с законом «О связи»)? Что понимается под универсальной услугой?

а) IP-телефония

б) видео

в) факс и IP-телефония

г) телефонная связь с использованием таксофонов, передача данных и предоставление доступа к сети «Интернет» с использованием пунктов коллективного доступа

5) В поле данных кадра X.25 входит какая информация?

а) заголовок сетевого уровня

б) сообщение транспортного уровня

в) пакет сетевого уровня – заголовок сетевого уровня и блок данных верхних уровней

г) кадр второго уровня

6) В заголовок какого типа кадра входит параметр номер ожидаемого информационного кадра X.25?

а) Супервизорный кадр отрицательной квитанции (REJ)

б) Ненумерованный кадр

в) Супервизорный кадр положительной квитанции (RR)

г) Кадр положительной квитанции (RR), кадр информационный

7) Со станции А на станцию В поступает информационный кадр сети X.25 «I». Что означает нумерация N(S) и N(R), входящая в заголовок этого кадра? Назначение этих параметров

а) N(S) – номер кадра, присвоенный на станции В, N(R) – номер ожидаемого информационного кадра на станции А

б) N(S) – номер кадра, присвоенный на станции А, N(R) – номер кадра ожидаемый на приеме станцией В

в) N(S) – номер кадра, присвоенный на станции В, N(R) – номер кадра, ожидаемый на станции В

г) N(S) – номер кадра, присвоенный на станции А, N(R) – номер кадра, ожидаемый на станции А

8) Приведена временная последовательность кадров X.25 между A и B.

- A отправляет информационный кадр «I» с параметрами N(S)=3, N(R)=17
- B, получив I(3,17), отправляет положительную квитанцию RR с параметром N(R)=4
- A, получив RR(4), отправляет I(4,17)
- B, получив I(4,17), отправляет I(17,x)
- A, получив I(17,x), отправляет I(y,z)

Ни один из этих кадров в канале не искажен. Чему равны x, y, z?

а) x=4, y=5, z=17

б) x=5, y=5, z=18

в) x=4, y=4, z=17

г) x=5, y=5, z=17

9) Приведена временная последовательность кадров X.25 между A и B.

- A отправляет информационный кадр “I” с параметрами N(S)=2, N(R=5)

B, получив I(2, 5), отправляет I(5, 3)

A, получив I(5, 3), отправляет I(3, 6), который искажается в канале

B отправляет I(6, 3)

A, получив I(6, 3), отправляет I(4, 6)

- B, получив I(4, 6), отправляет REJ (x)
- A, получив REJ (x), отправляет I(y, z)

Чему равны параметры x, y, z?

а) x=4, y=4, z=7

б) x=3, y=3, z=7

в) x=2, y=4, z=6

г) x=3, y=4, z=7

10) Каким основным принципам должны придерживаться разработчики фоновых программ станций коммутации сетей связи?

а) экономия машинного времени

б) обработка фоновыми программами очередей сообщений, находящихся в различных областях оперативной памяти

в) деление больших ветвей программ с целью упрощения отладки и модернизации ПО

г) иерархический принцип построения программного обеспечения (программы, подпрограммы)

11) Сколько команд потребуется для снятия с очереди к фоновой программе первого кадра X.25 при условии, что в очереди больше одного кадра?

а) 1 команда.

-число кадров в характеристике очереди уменьшить на 1.

б) 3 команды.

- уменьшить число кадров в характеристике очереди на 1
- заменить адрес первого кадра в характеристике очереди на адрес следующего в очереди кадра
- в кадре, ставшим первым, установить в 0 поле, указывающее на адрес предыдущего кадра в очереди

в) 2 команды.

- заменить адрес первого кадра в характеристике очереди на адрес следующего в очереди кадра
- уменьшить число кадров в характеристике очереди на 1

г) 2 команды.

- заменить адрес первого кадра в характеристике очереди на адрес следующего в очереди кадра
- В кадре, ставшем первым, установить в 0 поле, указывающее на адрес предыдущего кадра в очереди

12) Сколько команд потребуется для установки в конце очереди одного кадра при условии, что в очереди больше одного кадра?

а) 1 команда. Число кадров в характеристике очереди увеличить на 1.

б) 5 команд.

- число кадров в характеристике очереди увеличить на 1
- адрес устанавливаемого кадра поставить в поле последнего кадра X.25 характеристики очереди
- адрес устанавливаемого кадра поставить в соответствующее поле предыдущего кадра очереди (в котором ранее был 0)
- адрес предыдущего кадра поставить в соответствующее поле устанавливаемого кадра
- соответствующее поле устанавливаемого кадра, указывающее на то, что он последний, поставить в 0

в) 3 команды.

- число кадров в характеристике очереди увеличить на 1
- адрес устанавливаемого кадра поставить в соответствующее поле предыдущего кадра очереди (в котором ранее был 0)
- адрес предыдущего кадра поставить в соответствующее поле устанавливаемого кадра

г) 2 команды.

- число кадров в характеристике очереди увеличить на 1

адрес предыдущего кадра поставить в соответствующее поле устанавливаемого кадра

13) Какая фоновая программа устанавливает состояние перехода в режим «передача отрицательной квитанции (REJ)»?

а) программа передачи кадров с буфера «I» кадров по таймеру

б) программа приема кадра «неготовность к приему» (RNR)

в) программа «обработка принятого «I» кадра»

г) программа передачи «I» кадра в канал

14) Сколько команд предоставляется фоновым программам при передаче в канал одного кадра длиной X.25 256 байт (скорость канала 64 Кбит/с, время исполнения одной команды 1 мкс)? Приведите расчёт.

а) ~ 1000 команд

б) ~ 10000 команд

в) ~ 100000 команд

г) ~ 30000 команд

15) Какая фоновая программа устанавливает режим «Подготовка к передаче положительной квитанции RR»?

а) Подготовка к передаче очередного «I» кадра с $О_{повт}$ по таймеру

б) Передача кадра отрицательной квитанции REJ

в) Обработка принятого кадра отрицательной квитанции REJ

г) Обработка принятого кадра «I»

16) Какая программа устанавливает режим «Передача «I» кадров с $О_{повт}$ по REJ»? Опишите условия формирования этого режима.

а) Обработка принятого кадра «I»

б) Обработка принятого кадра отрицательной квитанции REJ

в) Установление и снятие запрета на передачу «I» кадров

г) Передача кадра отрицательной квитанции REJ

17) Какой недостаток постоянного виртуального канала (ПВК) по сравнению с коммутируемым виртуальным каналом? Приведите процедуру формирования ПВК.

а) Больше время восстановления ПВК при неисправности канала связи

б) Меньше величина задержки сообщения

в) Дороже

г) Больше вероятность потерь пакетов

18) На каком уровне стека протоколов модели OSI производится коммутация пакетов «Данные» X.25 по коммутируемому виртуальному каналу?

а) первом

б) втором

в) третьем

г) четвертом

19) На каком уровне стека протоколов производится коммутация кадров сети Frame Relay и ячеек сети ATM по постоянному виртуальному каналу?

а) первом

б) втором

в) третьем

г) четвертом

20) В чем недостаток сквозного шифрования в сети пакетной коммутации?

а) открытые сообщения в центре коммутации пакетов (ЦКП)

б) открытые сообщения на абонентском участке

в) угроза анализа трафика

г) открытие сообщения между ЦКП

21) В чем недостаток канального шифрования в сети пакетной коммутации?

а) открытие сообщения на абонентском участке

б) открытие сообщения в ЦКП

в) открытие сообщения между ЦКП

г) угроза анализа трафика

22) Какая функция использования комбинированного шифрования (канального и сквозного) в сети передачи данных пакетной коммутации?

а) защита от атаки «анализ трафика»

б) защита от раскрытия информационной части пакета

23) Какая функция по установлению соединений программ сетевого уровня X.25 при обработке пакетов «Запрос Вызова» и «Вызов Принят» ?

а) установление комбинированного виртуального канала

б) установление постоянного виртуального канала (ПВК)

в) установление коммутируемого виртуального канала (КВК)

24) Какая функция по маршрутизации программ сетевого уровня X.25 при обработке принятых пакетов «Запрос Вызова» и «Вызов Принят»?

а) коммутация пакетов сетевого уровня

б) восстановление потерянных пакетов сетевого уровня

в) формирование таблицы маршрутизации пакетов X.25 по логическим канальным номерам LCN для создания виртуального канала

г) передача пакетов на канальный уровень

25) Какое максимальное число пакетов X.25 «Запрос Вызова» может быть установлено в очереди на передачу в канальные процессоры, подключенные к центральному процессору ЦКП?

а) По числу канальных процессоров

б) Произведение числа канальных процессоров, умноженное на 2

в) 4094

г) 1047

26) Какое число команд (ориентировочно) в диспетчере программ и чем оно определяется?

а) 2000; б) 10000; в) 200; г) 20000.

27) Какие показатели QoS для речи и видео являются основными?

а) вариация задержки (jitter)

б) максимальная величина задержки

в) средняя скорость передачи и согласованный (максимальный) объем пульсации

г) коэффициент потери кадров (ячеек, пакетов)

28) Какая фоновая программа устанавливает состояние режим «Подготовка к передаче в канал кадра REJ»?

а) прием «I» кадра с канала

б) прием кадра положительной квитанции RR

в) прием кадра отрицательной квитанции REJ

29) Где содержится адрес первого кадра в очереди к фоновой программе?

а) в первом кадре очереди

б) в последнем кадре очереди

в) в характеристике очереди.

30) Где содержится информация о числе кадров в очереди к фоновой программе?

а) в последнем кадре очереди

б) в характеристике очереди

в) в первом кадре очереди

31) В каком варианте передача информационного кадра из буфера повтора производится всегда?

а) при приёме информационного кадра

б) при приёме кадра отрицательной квитанции REJ

в) при приёме кадра положительной квитанции RR

32) Какие типы кадров из буфера повтора передаются? Варианты ответов:

а) информационные

б) отрицательной квитанции REJ

в) положительной квитанции RR

33) Какой показатель QoS для передачи данных является основным?

а) вариация задержки (jitter)

б) максимальная величина задержки

в) средняя скорость передачи и согласованный (максимальный) объем пульсации

г) коэффициент потери кадров (ячеек, пакетов)

34) Какая фоновая программа устанавливает режим «Подготовить к передаче в канал кадра RR»?

а) программа приёма кадра REJ

б) программа приёма кадра RR

в) программа приёма информационного кадра

35) Какая фоновая программа снимает режим «Подготовить к передаче в канал кадра REJ»?

а) программа приёма кадра REJ

б) программа приёма кадра RR

в) программа передачи кадра REJ

36) В сетях Frame Relay и ATM по какому каналу производится процедура сигнализация при установлении КВК?

а) По тому же виртуальному каналу, что и передача информационных сообщений (фреймов, кадров)

б) По физическому каналу

в) По каналу транспортного уровня – протоколу TCP

г) По выделенному виртуальному каналу

37) Какой параметр по протоколу сети Frame Relay, определяющий качество обслуживания QoS, не входит в сообщение пользователя на установление КВК (в сообщение SETUP)?

а) согласованная информационная скорость

б) согласованный объем пульсации

в) время задержки кадра

г) дополнительный объем пульсации

38) На каком уровне стека протоколов осуществляется коммутация в сети Frame Relay и в сети X.25?

а) на уровне 3

б) на уровне 2

в) на уровне 1

39) На каких типах виртуальных каналов Frame Relay и ATM формируется виртуальная частная сеть (VPN)?

а) коммутируемый виртуальный канал (SVC)

б) постоянный виртуальный канал (PVC)

в) коммутируемый постоянный канал (SPVC)

г) SVC или PVC

40) В чем преимущество коммутируемого постоянного виртуального канала SPVC (в сетях Frame Relay и ATM) перед постоянным виртуальным каналом?

а) меньше вероятность потерь пакетов

б) меньше задержка сообщений

в) быстрее восстановление виртуального соединения при неисправности канала связи между коммутаторами

г) большая пропускная способность виртуального соединения

41) Какой из перечисленных аспектов сравнения показателей QoS и SLA правильный? Приведите пример одного из показателей SLA, которого нет в QoS.

а) число показателей QoS больше, чем SLA

б) QoS предусматривает в качестве одного из показателей информационную безопасность

в) SLA предусматривает заключение письменного соглашения между пользователем и поставщиком услуг

г) SLA предусматривает согласование требований по качеству обслуживания при установлении каждого соединения между пользователями.

42) Какой параметр синусоидальной несущей изменяется в большинстве модемов каналов тональной частоты для передачи максимального количества бит в одном боде?

а) амплитуда

б) фаза

в) частота

г) комбинация амплитуды и фазы

43) Какую фунцию не выполняет модем?

а) преобразование аналогового сигнала в цифровой

б) преобразование цифрового сигнала в аналоговый

в) повышение надежности канала связи

г) повышение скорости передачи

44) В какой глобальной сети связи обеспечивается выполнение требований пользователя по обеспечению конкретного значения показателя качества речи, видео, данных?

а) Frame Relay

б) ATM

в) ISDN

г) X.25

45) Какую функцию выполняет байт циклического кода в ячейке ATM?

а) исправление одиночных ошибок в информационном поле ячейки

б) исправление одиночных ошибок в четырех байтах заголовка, обнаружение некоторых групповых ошибок и синхронизация ячеек

в) обнаружение ошибок в четырех байтах заголовка

г) обнаружение ошибок в заголовке ячеек

46) В каких технологиях первичных сетей связи используется принцип частотного разделения?

а) PDH (плезиохронная цифровая иерархия)

б) SDH (синхронная цифровая иерархия)

в) DWDM (уплотнение волнового мультиплексирования)

47) Какой примерно процент составляют одиночные ошибки в волоконно-оптических каналах?

а) 55

б) 35

в) 95

г) 5

48) Какие одинаковые показатели QoS предусмотрены в технологиях Frame Relay и ATM?

а) вариация задержки (jitter)

б) максимальная величина задержки

в) средняя скорость передачи и согласованный (максимальный) объем пульсации

г) коэффициент потери кадров (ячеек)

49) Чем лучше VPN-ATM по сравнению с VPN-FR?

а) устанавливается не только на основе коммутируемого виртуального канала

б) устанавливается не только на основе постоянного виртуального канала

в) ATM предоставляет высокое качество обслуживания для мультимедийных служб при соответствующем требовании пользователя

50) Какие недостатки технологии первичных сетей PDH были учтены и преодолены разработчиками технологии SDH?

а) невозможность непосредственного выделения данных низкоскоростного канала из данных высокоскоростного канала

б) отсутствие встроенных средств управления отказоустойчивостью, конфигурацией, качеством, информационной безопасностью

в) низкие скорости передачи данных

51) Какое максимальное число пользователей телефонной службы могут быть соединены через один узел коммутации ATM при скорости канала несколько Тбит/с?

а) $2^{1} \approx 6,5^{6} м$

б) $2^{2} \approx 1,8^{4} м$

в) $2^{2} \approx 6,1^{6} м$

г) $2^{2} \approx 2 \quad ,4 м$

52) Какую функцию выполняют уровни адаптации ATM (AAL)?

а) обеспечивают работу только с трафиком данных

б) обеспечивают работу только с изображениями

в) обеспечивают работу только с аудио

г) обеспечивают работу со всеми приведенными выше видами трафика

53) Какие виды адресации используются при переносе данных в IP-сети?

а) только глобальный IP-адрес

б) только локальный адрес подсети

в) глобальный IP-адрес сети и локальный адрес подсети

54) Какой недостаток VPN-IPSec?

а) нет защиты от угроз «анализ трафика»

б) не обеспечивает ИБ от дешифрирования сообщения

в) не обеспечивает QoS пользователям

г) не защищает от несанкционированного доступа

55) От какой угрозы ИБ нет защиты в транспортном режиме IPSec? Варианты ответов:

а) дешифрование данных

б) «анализ трафика»;

в) дешифрование IP-адреса оконечного пункта.

56) Какие стадии предшествуют и создают защищенную связь при работе протоколов ИБ?

а) управление ключами

б) аутентификацию, создание общего главного ключа, согласование протоколов ИБ и создание общих ключей

в) согласование протоколов ИБ и создание общих ключей

57) Какая защита открытых параметров предусмотрена от угрозы «человек посередине» в протоколе TLS при использовании метода Диффи-Хеллмана для создания защищенной связи?

а) передача открытых параметров в составе сертификата

б) шифрование открытым ключом получателя по алгоритму RSA

в) подпись закрытым ключом отправителя хеш-кода по алгоритму RSA

б) аутентификацию, создание общего главного ключа, согласование протоколов ИБ и создание общих ключей

в) согласование протоколов ИБ и создание общих ключей

58) От какой угрозы предусмотрена защита ИБ при маршрутизации в IP-сети ?

а) взлом таблицы маршрутизации

б) просмотр данных

в) создание и передача нелегитимных сообщений обновления таблиц маршрутизации

59) Какой основной недостаток модели интегрированного обеспечения качества обслуживания IntServ?

а) не позволяет использовать в системе с большим числом потоков информации

б) сложная реализация алгоритма

в) обеспечивает ограниченное число показателей качества обслуживания

60) При модели дифференцированного обеспечения качества обслуживания DiffServ и схеме гарантированной пересылки, какое предусмотрено число классов приоритета обслуживания и классов сброса пакетов при перегрузке для каждого приоритета обслуживания?

а) четыре класса приоритета обслуживания и три класса сброса

б) три класса приоритета обслуживания и четыре класса сброса

в) пять классов приоритета обслуживания и четыре класса сброса

г) четыре класса приоритета обслуживания и пять классов сброса

61) Какие характеристики качества обслуживания не приняты для IP – сетей в рекомендации МСЭ-Т Y.1541?

а) задержки в доставке пакета

б) вариация задержки (jitter)

в) коэффициент готовности доступа к сети

г) коэффициент потери и коэффициент ошибок пакетов

62) В технологии какой сети не реализовано установление соединения с определенными показателями QoS, запрашиваемыми пользователем?

а) ATM

б) Internet

в) MPLS

63) В какой технологии сети связи отсутствует фаза установления каждого соединения перед фазой передачи данных?

а) ATM

б) ISDN

в) MPLS

г) Internet

64) Какие службы обеспечивают MPLS?

а) речь и видео

б) речь и передача данных

г) речь, видео и передача данных

65) Абоненты каких сетей могут быть подключены к сети MPLS?

а) IP-сети

б) IP-сети и ATM

в) IP-сети, Ethernet, ATM, Frame Relay

66) Что общего между MPLS и ATM, Frame Relay?

а) отсутствует режим постоянного виртуального канала

б) устанавливается соединение с помощью уникальных идентификаторов пакетов, отличающихся на входе и выходе коммутатора

в) отсутствует режим коммутируемого виртуального канала

67) В каком устройстве сети MPLS впервые устанавливается метка?

а) в маршрутизаторе LSR

б) в брандмауэре

в) в маршрутизаторе LER

68) Что представляет собой тракт LSP сети MPLS?

а) последовательность меток в маршрутизаторах, расположенных на пути следования потока данных от отправителя получателю

б) таблицы маршрутизации в узлах коммутации, содержащие физические адреса отправителя и получателя

в) таблицы маршрутизации в граничных маршрутизаторах LER

69) Для чего производится замена меток в маршрутизаторе сети MPLS?

а) повысить надежность передачи пакетов

б) выполнить требование пользователя по пропускной способности тракта;

в) создать коммутируемый по меткам тракт LSP

70) Сколько классов гарантированного обслуживания поддерживает модель DiffServ и сколько сеть MPLS в соответствии со стандартным полем заголовка метки?

а) 12 (DiffServ), 8(MPLS);

б) 10 (DiffServ), 8(MPLS);

в) 14 (DiffServ), 3(MPLS)

71) Какие функциональные возможности использует стек заголовка метки MPLS?

а) объединение нескольких LSP в один (агрегирование)

б) быстрая ремаршрутизация

в) создание VPN

72) Какой протокол транспортного уровня использует в сети MPLS протокол распределения меток LDP?

а) UDP

б) TCP

в) UDP и TCP

73) Что общего при использовании TE-туннеля в MPLS и постоянного виртуального канала в сетях ATM и Frame Relay?

а) централизованное задание маршрута

б) обеспечение высокой пропускной способности

в) создание виртуальной частной сети

74) Какие протоколы в сети MPLS используются для обеспечения инжиниринга трафика?

Варианты ответов:

а) расширенный OSFP

б) расширенный RSVP

75) Какое в сети MPLS время восстановления пути при быстрой ремаршрутизации?

а) 300мсек

б) 150мсек

в) 50мсек

г) 250мсек

76) Какое из перечисленных преимуществ MPLS перед IP-сетью не имеет место?

а) QoS;

б) TE;

в) FRR;

г) VPN;

д) все перечисленные преимущества имеют место.

77) Чем отличается маршрутизатор коммутации меток LSR от граничного маршрутизатора?

а) LSR выполняют только функции коммутации по метке, а LER должен также поддерживать обычную маршрутизацию (например, по IP – адресу)

б) Путь переноса пакета проходит только через LSR, а через LER - нет

в) LER содержит метку, а LSR - нет

г) LSR содержит метку, а LER - нет

78) Какое поле в заголовке MPLS отсутствует?

(приведите пример использования стека)

а) метка

б) бит, указывающий на то, что является ли метка последней в стеке или нет

в) открытый ключ шифрования

г) класс качества обслуживания QoS

79) Таблица маршрутизации VRF виртуальной частной сети VPN третьего уровня MPLS (MPLS L3VPN) создаётся сообщениями между какими маршрутизаторами?

а) CE-PE

б) P- PE, PE-PE

в) PE-PE, CE-PE

г) P-PE

80) Глобальная таблица маршрутизация MPLS L3VPN создаётся сообщениями между какими маршрутизаторами (и на основе каких протоколов)?

а) CE-PE

б) P- PE, PE-PE

в) PE-PE, CE-PE

г) P-PE

81) На какой технологии сети связи требуется обязательно шифрование для создания виртуальной частной сети (VPN)?

а) MPLS

б) IP – сети

в) Frame Relay

г) ATM

82) Каким образом создается туннель для формирования MPLS L3VPN?

а) с помощью стека меток

б) шифрованием метки

в) шифрованием поля данных

83) В чем нет преимущества MPLS L3VPN перед VPN на базе протокола IP-Sec?

а) в выполнении требований по обеспечению QoS

б) в масштабируемости

в) в уровне обеспечения ИБ

г) в сложности при установке и управлении стоимости создания VPN

84) На какие две группы можно разделить все типы алгоритмов шифрования?

а) шифрование с общим ключом и блочные коды

б) шифрование с открытым ключом и поточные шифры

в) шифрование с общим ключом и шифрование с открытым ключом

85) Какой математический аппарат положен в основу криптографии с открытым ключом по алгоритму RSA?

а) дифференциальное исчисление и модульная арифметика

б) интегральное исчисление и модульная арифметика

в) односторонние функции и модульная арифметика

г) арифметика в остаточных классах и интегральное исчисление

86) Какие способы защиты ИБ могут отсутствовать в сообщении с электронно-цифровой подписью?

а) аутентификация источника сообщения

б) шифрование сообщения

в) целостность данных сообщения

г) неотказуемость источника сообщения в отправлении принятого сообщения

87) Каким ключом шифруется хеш-код (профиль) сообщения при создании электронно-цифровой подписи (ЭЦП) и дешифруется на приеме (Каким образом производится проверка подлинности ЭЦП)?

а) шифруется закрытым ключом получателя, дешифруется открытым ключом получателя

б) шифруется закрытым ключом отправителя, дешифруется открытым ключом отправителя

в) шифруется открытым ключом получателя, дешифруется открытым ключом получателя

г) шифруется закрытым ключом отправителя, дешифруется открытым ключом получателя

88) Каким ключом шифруется общий ключ симметричного шифрования для передачи в сеть и дешифруется получателем на приеме?

а) шифруется закрытым ключом получателя, дешифруется открытым ключом получателя

б) шифруется закрытым ключом отправителя, дешифруется открытым ключом отправителя

в) шифруется открытым ключом получателя, дешифруется закрытым ключом получателя

г) шифруется закрытым ключом отправителя, дешифруется открытым ключом получателя

89) Какая характеристика не входит в защищенную связь протокола IPSec? Варианты ответов:

а) идентификатор протокола защиты – AH или ESP

б) параметр режима – транспортный или туннельный

в) параметр качества обслуживания – задержка или вероятность потери пакета

г) максимальный размер пакета

90) Какой режим IPSec используется для создания VPN?

а) только транспортный

б) транспортный или туннельный

в) только туннельный

91) Согласно рекомендации международного союза электросвязи Е.408 (Требования к безопасности сети связи) какие количественные характеристики относятся к угрозе ИБ и соответствующему риску ИБ?

а) вероятность угрозы

б) последствия воздействия угрозы

в) способ защиты

г) вероятность угрозы и последствия воздействия угрозы

92) Какой тип коммутации используется в сети ISDN?

а) коммутация каналов

б) коммутация меток

в) коммутация пакетов

93) Какой тип коммутации используется в сети доступа ISDN (DSS1)?

а) коммутация каналов

б) коммутация меток

в) коммутация пакетов

94) Какой тип коммутации используется в ОКС№7 сети ISDN?

а) коммутация каналов

б) коммутация меток

в) коммутация пакетов

95) Что понимается под термином *сигнализация* в сетях связи в соответствии с рекомендацией международного союза электросвязи Q.9? Варианты ответов:

а) управление сетью связи

б) сообщение о нарушении работы сети (перегрузка, неисправность канала связи, нарушение таблицы маршрутизации, атака злоумышленника DoS или «отказ в обслуживании», нарушение функционирования части сети связи и др.)

в) обмен неречевой информации, которая выполняет функцию установления, разрыва и управления вызовом, а также управление сетью в автоматизированном телекоммуникационном оборудовании.

96) В чем заключается основная задача сертификата?

а) обеспечить секретный обмен открытыми ключами пользователя, связав открытый ключ пользователя с именем пользователя

б) обеспечить секретный обмен закрытыми ключами пользователя

в) убедиться в подлинности открытого ключа получателя

г) обеспечить выполнение аутентификации (подлинность источника информации)

97) Какое значение входит в состав сертификата пользователя?

а) зашифрованный открытый ключ

б) зашифрованный закрытый ключ

в) незашифрованный открытый ключ

98) Какую функцию выполняет цепочка сертификатов?

а) формирует каталог открытых ключей пользователей

б) позволяет одному пользователю проверить достоверность открытого ключа другого пользователя, сертификат которого получен в другом центре сертификации

в) получить пользователю зашифрованный открытый ключ другого пользователя

99) Сколькими сообщениями обмениваются при успешной аутентификации объекты сети ISDN в конфигурации центров сертификации стандарта ETSI ETS 300 841?

а) 5

б) 4

в) 3

100) Какие сертификаты пересылает объект в первом и втором сообщении в стандарте ETSI ETS 300 при аутентификации в сети ISDN?

а) GCA<<Cx>>, Cx<<X>> в первом сообщении и GCA<<C_Y>>, C_Y<<Y>> во втором сообщении

б) GCA<<C_Y>>, Cx<<X>> в первом сообщении и GCA<<C_Y>>, C_Y<<Y>> во втором сообщении

в) GCA<<C_Y>>, Cx<<X>> в первом сообщении и GCA<<C_Y>>, C_Y<<X>> во втором сообщении

101) Правильный прием каких основных показателей свидетельствует об успешной аутентификации объекта сети ISDN в соответствии со стандартом ETSI ETS 300 841?

а) достоверный открытый ключ объекта, идентификатор объекта, общий ключ

б) достоверный открытый ключ объекта, идентификатор объекта, показатель защиты от угрозы «повтор»

в) достоверный открытый ключ объекта, общий ключ, показатель защиты от угрозы «повтор»

102) В каких сетях связи не используется ОКС№7?

а) ТфОП/ISDN

б) MPLS

в) Интеллектуальная сеть связи

г) GSM

103) К какому уровню OSI относится подсистема передачи сообщений (MTP) ОКС№7?

а) сетевому

б) канальному и сетевому

в) физическому, канальному и сетевому

104) На каком уровне MTP осуществляется контроль за качеством звена сигнализации (канала передачи данных)?

а) первом

б) втором

в) третьем

105) На какие две основные функции подразделяется уровень 3 подсистемы MTP?

а) маршрутизация и управление сетью сигнализации

б) распознавание и распределение сигнальных сообщений

в) распределение сообщений и обработка сигнальных сообщений

г) обработка сигнальных сообщений и управление сетью сигнализации

106) Какое значение требования к MTP в части суммарного времени неготовности пучка маршрутов сигнализации ОКС№7?

а) 1 час в год

б) 2 часа в год

в) 0,5 часа в год

г) 10 мин. в год

107) Какой протокол не относится к сигнализации в сети ТфОП?

а) SIP

б) RTP

в) H.323

108) Какое устройство не относится к сети SIP?

а) Агент пользователя UA

б) прокси-сервер

в) маршрутизатор

г) регистратор

д) сервер переадресации

109) Какие виды краж идентификатора являются угрозами фрода (использование услуг связи без их оплаты) в сети SIP?

а) кража идентификатора другим пользователем-нарушителем, который начинает пользоваться всеми услугами легитимного пользователя мобильность устройств пользователя

б) кража подписки

в) создание запросов многоадресной связи с фальсифицированными IP-адресами источника запроса

110) Какие виды сообщений в сети SIP?

а) запрос, ответ

б) регистрация, запрос вызова

в) регистрация, переадресация

111) Какой адрес всегда входит в поле *To* сообщения INVITE?

а) глобальный адрес AoR вызываемого пользователя

б) текущий адрес вызываемого пользователя

в) адрес сервера местоположения пользователя

112) Каким образом производится сопряжение ОКС№7 с сетью SIP?

а) замена адресов пунктов сигнализации ОКС№7 на адреса сети SIP и наоборот

б) инкапсуляция ISUP в тело запросов SIP

в) замена адресов пунктов сигнализации ОКС№7 на адрес сервера местоположения пользователя и наоборот

113) Какие из приведенных мер злоумышленника могут привести к атаке DoS в сети SIP?

а) ненадежная аутентификация при запросе регистрации

б) создание запросов многоадресной связи с фальсифицированными IP-адресами источника запроса

в) замена адресов пунктов сигнализации ОКС№7 на адрес сервера местоположения пользователя и наоборот

г) передача ложных сообщений управления сетью сигнализации ОКС№7

114) Механизм ИБ какого уровня эталонной модели TCP/IP не используется в сети SIP?

а) прикладного

б) транспортного

в) межсетевого

г) уровня сетевого доступа

115) Какой протокол шифрования и аутентификации используется при транспортировке данных в сетях VoIP?

а) AES, HMAC

б) DES, ЭЦП

г) AES, ЭЦП

116) Какой механизм шифрования и аутентификации используется в сети сигнализации SIP?

а) TLS

б) S/MIME

в) HTTP Digest Authentication

г) PGP

117) Какой параметр включает сообщения управления сетью сигнализации ОКС№7 - перевод трафика на резервное звено сигнализации COO и возврат трафика с резервного звена сигнализации COA?

а) номер исходящего пункта сигнализации

б) номер пункта сигнализации назначения

в) последняя успешно принятая значащая сигнальная единица MSU

118) Какую функцию не выполняет пункт сигнализации ОКС№7 при получении сообщения управления сетью сигнализации TFP (вынужденная ремаршрутизация)?

а) останавливается перенос сигнального трафика по недоступному сигнальному маршруту номер исходящего пункта сигнализации

б) определяется резервный сигнальный маршрут номер пункта сигнализации назначения

в) перенос сигнального трафика на резервное звено сигнализации

г) перенос сигнального трафика на резервный маршрут

119) Какое значение включает сообщение управления сетью сигнализации (COO) перевода трафика ОКС№7 с неисправного звена сигнализации на исправное?

а) признак неисправности звена сигнализации

б) номер неисправного звена сигнализации

в) номер последней успешно принятой значащей сигнальной единицы MSU с противоположной стороны звена сигнализации

120) Какое значение включает сообщение управления сетью сигнализации (TFP) вынужденной ремаршрутизации?

а) адрес недоступного пункта сигнализации

б) идентификатор недоступного пункта сигнализации

в) время недоступности пункта сигнализации

121) Какое значение включает сообщение управления сетью сигнализации (TFC) управляемого переноса?

а) адрес недоступного пункта сигнализации

б) идентификатор недоступного пункта сигнализации

в) адрес пункта сигнализации, указывающего на его состояние перегрузки

122) Какие причины вызывают необходимость перезапуска MTP?

а) изоляция пункта сигнализации от сети из-за недоступности к нему всех звеньев сигнализации

б) неисправность пункта сигнализации

в) перегрузка пункта сигнализации

123) Какие подсистемы пользователя ОКС№7 относятся к интеллектуальной сети?

а) SCCP

б) MAP

в) INAP

г) INAP и TCAP

124) Какие функции ОКС№7 не выполняет подсистема управления соединением сигнализации SCCP?

а) выбор канала связи для обмена информацией

б) обеспечивает работу служб передачи данных без установления соединения и служб с установлением соединений

в) осуществляет расширение адресации

г) обеспечивает гибкие механизмы управления маршрутизацией с использованием номера подсистемы SSN, глобального заголовка GT

125) Сколько сообщений в интеллектуальной сети требуется для взаимной аутентификация абонента-роумера и гостевой UPT-системы?

а) 4

б) 5

в) 3

г) 6

126) Какой вид множественного доступа используются в GSM?

а) FDMA (Frequency Division Multiple Access) – множественный доступ с разделением каналов по частоте

б) TDMA (Time Division Multiple Access) – множественный доступ с разделением каналов по времени;

в) CDMA (Code Division Multiple Access) – множественный доступ с кодовым разделением каналов

г) OFDMA (Orthogonal Frequency Division Multiple Access) - ортогональный множественный доступ с частотным разделением

д) TDMA/FDMA

127) Какая подсистема не входит в архитектуру GSM?

а) подсистема информационной безопасности

б) подсистема радиосвязи

в) подсистема сетей и коммутации

г) операционная подсистема

128) Какое максимальное количество каналов могут обслуживаться (теоретически) одной базовой станцией GSM?

а) 124

б) 1024

в) 992

г) 256

129) Понятие многолучевого отражения на радиоучастке GSM и в чем оно проявляется?

а) сильное затухание сигнала

б) межсимвольная интерференция

в) слабое затухание сигнала

130) Какой основной принцип системы сотовой связи GSM?

а) высокая помехозащищенность

б) мягкий роуминг

в) повторное использование частот

131) Сколько временных слотов содержится в одном кадре TDM в GSM?

а) 7

б) 26

в) 8

г) 4

132) Какая база данных GSM позволяет определить местоположение мобильной станции?

а) VLR

б) HLR

в) AUC

г) EIR

133) Какая база данных GSM содержит данные об абоненте-роумере?

а) VLR

б) HLR

в) AUC

г) EIR

134) Какая величина показателей кодека речи GSM по скорости передачи информации и оценке MOS?

а) 13 Кбит/с; 3,58

б) 64 Кбит/с; 3,58

в) 13 Кбит/с; 4,12

г) 64 Кбит/с; 4,12

135) Сколько бит исправляют в GSM коды с прямой коррекцией FEC?

а) 5

б) 4

в) 2

г) 1

136) Что означает скорость кодирования?

а) избыточность, вносимая кодированием и равная отношению длины исходной информации к длине информации, передаваемой в канал

б) максимальная пропускная способность канала связи

в) средняя пропускная способность канала связи

137) Какую цель преследует процедура перемежения в сотовых сетях связи?

а) уменьшение помех на участке радиодоступа

б) преобразование групповых ошибок сообщений в канале в одиночные и последующее их исправление с помощью корректирующих кодов

в) обнаружение групповых ошибок сообщений в канале

г) обнаружение одиночных и двойных ошибок сообщений в канале

138) Какой вид шифрования/дешифрования используется на радиоучастке GSM?

а) поточное

б) блочное

в) криптография с открытым ключом

139) Какую функцию выполняет значение номера кадра при шифровании на радиоучастке GSM?

а) сокращение задержки при шифровании

б) повышение уровня безопасности при шифровании

в) позволяет реализовать поточное шифрование

140) Какая аутентификация предусмотрена в GSM?

а) пользователя

б) сети

в) взаимная

141) Ниже приведена последовательность операций по регистрации абонента-роумера при несовпадении TMSI мобильной станции и сети. Между какими шагами нарушена правильная последовательность?

а) по значению LAI определяется поиск местоположения гостевого регистра VLR предыдущей области обслуживания абонента-роумера

б) производится аутентификация станции абонента-роумера

в) пересылка TMSI и других параметров из гостевого регистра VLR предыдущей области обслуживания абонента-роумера в текущий VLR

г) запись в мобильную станцию новой LAI и TMSI

142) Какие функции из перечисленных являются общими в сигнализации SIP и в сети GSM?

а) мобильность устройств пользователя

б) изменяемый адрес вызываемого пользователя

в) возможность установления широковещательной и многоадресной связи

143) Рассматривается случай запроса регистрации пользователем GSM при несовпадении значения TMSI в текущем регистре VLR с TMSI в мобильной станции. Какой этап регистрации из перечисленных неверный?

а) на основании полученного от пользователя идентификатора области местоположения пользователя (LAI) определяется VLR, который ранее обслуживал данную мобильную станцию

б) устанавливается соединение текущего VLR с VLR предыдущей области обслуживания

в) текущий VLR передает в предыдущий VLR значение IMSI пользователя

г) предыдущий VLR передает в текущий VLR параметры пользователя, в том числе TMSI.

144) На каких участках сети в GSM не используются сообщения ОКС№7 прикладного уровня MAP?

а) между шлюзом GMSC и регистром HLR при поступлении вызова к мобильной станции извне (например, ТфОП)

б) между гостевыми регистрами VLR при роуминге

в) между коммутаторами MSC при обмене данными

г) между гостевым и домашним регистрами при вызове абонента-роумера

145) Для какой цели в GSM используется роуминговый номер мобильной станции?

а) поиск местоположения текущего гостевого регистра в области обслуживания абонента-роумера

б) защита приватных данных местоположения абонента-роумера

в) аутентификация абонента-роумера

146) Какой уровень иерархии федеральной сети общего пользования GSM неверный?

а) уровень сетей отдельных операторов

б) уровень транзитной сети с локальным центром коммутации (ЛЦК)

в) уровень местной сети

г) уровень транзитной сети с транзитным центром коммутации (ТЦК)

147) Какой уровень иерархии сети связи общего пользования ТфОП неверный?

а) уровень междугородной сети связи

б) уровень транзитной сети

в) уровень местной сети

г) уровень международной сети

148) Какие сообщения подсистемы управления сетью сигнализации на сетевом уровне MTP ОКС№7 могут быть использованы злоумышленником для атаки DoS?

а) TFP, UPU, TFC, TFR, COO, ECO

б) TFC, TFR, COO, ECO

в) UPU, TFC

г) TFP

149) К последствиям отказа в установлении каких соединений не относятся атаки DoS ОКС№7 в результате фальсификации сообщений обновления маршрутизации?

а) между абонентами сети ТфОП/ISDN

б) между абонентами сети GSM

в) между абонентами сети ТфОП/ISDN и абонентами сети GSM

г) между абонентами сети Интернет

д) между абонентами IP-телефонии соединений через протокол SIP-T

150) На каких участках сетей ТфОП/ISDN и GSM выше риск ИБ в отношении последствий

отказа DoS в ОКС№7 из-за фальсификации сообщений обновления маршрутизации?

а) внутри самого высокого уровня иерархии сети

б) внутри самого низкого уровня иерархии сети

в) между смежными уровня иерархии сети

151) При какой скорости кодировании достигается максимальная скорость передачи в сети GPRS?

а) 1/2

б) 3/4

в) 2/3

г) 1

152) Что позволяет повысить скорость передачи в сети EDGE?

а) модем

б) метод перескока частоты

в) использование нескольких временных слотов

153) Что относится к недостаткам множественного доступа TDMA/FDMA по сравнению с множественным доступом CDMA?

а) дороговизна

б) отсутствие международного роуминга

в) жесткий роуминг

154) Что относится к преимуществу множественного доступа CDMA по сравнению с множественным доступом TDMA/FDMA?

а) более дешевая сеть

б) отношение «сигнал/шум» больше, что обеспечивает более высокое качество связи.

в) самая распространенная технология беспроводных сотовых сетей в мире

155) Что относится к преимуществу информационной безопасности сети UMTS по сравнению с GSM?

а) защита целостности данных

б) возможность гибкой смены фиксированных механизмов ИБ с целью усиления защиты

в) аутентификация односторонняя

г) аутентификация взаимная

156) Какой механизм шифрования используется в сети UMTS при аутентификации сети и обеспечении целостности сообщений?

а) электронно-цифровая подпись

б) никакой

в) шифрование и дешифрование с общим ключом

г) шифрование

157) Какой способ организации сети предусматривает стандарт IEEE 802.11?

а**)** режим беспроводной самоорганизующейся сети без точки доступа (Ad Hoc)

б) режим инфраструктуры (с точкой доступа)

в) режим Ad Hoc сети и режим с точкой доступа

158) Какие проблемы множественного доступа существуют в беспроводных сетях стандартов IEEE 802.11 по сравнению с проводной сетью Ethernet?

а**)** проблема скрытой станции

б) проблема засвеченной станции

в) проблема прихода обратно шумового всплеска

159) Какие функции выполняет подуровень управления доступом к среде MAC в беспроводных сетях стандартов IEEE 802.11?

а**)** какая станция будет передавать следующей

б) аутентификации пользователя

в) шифрования данных

г) способ передачи (перескок частоты, OFDM и др.)

160) Какое число антенн технологии многоканальных антенных систем MIMO может быть использовано в сети стандарта IEEE 802.11n?

а) 12

б) 6

в) 4

г) 3

161) Какой вид доступа используются в сети стандарта IEEE 802.11n?

а) OFDM

б) перескок частоты

в) CDMA

162) Какой из перечисленных способов обеспечения ИБ не предусмотрен в протоколе WEP в беспроводных сетях стандартов IEEE 802.11?

а) аутентификация пользователя

б) управление ключами

в) шифрование

г) целостность сообщений

163) Какую функцию не выполняет протокол EAP-TLS в беспроводных сетях стандартов IEEE 802.11?

а) установление мастер-ключа

б) установление сессионного ключа

в) установление ключа обеспечения целостности сообщений

г) взаимная аутентификация

164) Какой алгоритм шифрования сообщений используется в протоколе 802.11i в беспроводных сетях стандартов IEEE 802.11?

а) DES

б) RC4

в) AES

г) TDES

165) В чем в сети WiMAX основное различие режимов OFDM и OFDMA?

а) основное использование OFDM – модуляция на основе 256 номинальных поднесущих

б) основное использование OFDMA – использование OFDM не только для модуляции, но и для множественного доступа (мультиплексирование каналов)

в) число подканалов в OFDM больше , чем в OFDMA

166) Какая модуляция в режиме OFDMA сети WiMAX является обязательной?

а) QAM-64

б) QAM-16

в) BPSK

167) Какая скорость кодирования в режиме OFDMA сети WiMAX является обязательной?

а) ½

б) ¾

в) 1,0

168) Аутентификация какого устройства предусмотрена в стандарте мобильного доступа сети WiMAX 802.16e-2005?

а) абонентской станции

б) базовой станции

в) взаимная аутентификация

169) Сколько ключей TEK используется для шифрования трафика в сети WiMAX? Варианты ответов:

а) 1

б) 2

в) 3

г) 4

170) В чем состоит основная особенность самоорганизующихся беспроводных сетей связи?

а) автоматическое восстановление работоспособности сети при неисправности узла коммутации

б) автоматическое восстановление таблиц маршрутизации узлов коммутации сети

в) возможность в отсутствии централизованной инфраструктуры обмениваться данными любой паре находящихся в зоне радиопокрытия узлов сети

171) Какая беспроводная сеть не является самоорганизующейся сетью?

а) сенсорная

б) спутниковая

в) мобильная Ad Hoc сеть

г) mesh-сеть

д) автомобильная беспроводная сеть (VANET)

172) В какой области сенсорная сеть используется?

а) окружающая среда

б) телемедицина

в) чрезвычайные ситуации (пожары, катастрофы и др.)

г) военные операции

173) Какие атаки в самоорганизующихся сетях относятся к атакам DoS, нарушающим маршрутизацию?

а) черная дыра

б) серая дыра

в) атака Сибиллы

г) атаки, направленные на истощение сетевых ресурсов

д) сборный пункт

174) Какие механизмы ИБ позволяют создать общий секретный ключ для взаимодействующих через сеть связи двух узлов?

а) HMAC

б) RSA

в) AES

г) метод Диффи-Хеллмана

175) В чем отличие аутентификации сообщений от других видов аутентификации?

а) обеспечивает достоверность одного источника сообщений

б) обеспечивает достоверность источников сообщений двух взаимодействующих объектов в сети связи

в) обеспечивает достоверность источника сообщения и его целостность

176) Какие функции выполняет в сети протокол RADIUS?

а) защита приватных данных

б) аутентификация (authentication)

в) авторизация (authorization)

г) учет (accounting)

Принятые сокращения

3GPP, Third Generation Partnership Project - Альянс сотрудничества по сетям мобильной беспроводной сети третьего поколения партнерство в области технологий 3G

AAL, ATM adaptation layer - уровень адаптации ATM
Ad Hoc - целевый сети
ADSL, Asymmetric Digital Subscriber Line - асимметричная широкополосная цифровая абонентскиая линия
AES, Advanced Encryption Standard - улучшенный стандарт шифрования
ANM, Answer Message – ответ абонента
AODV, Ad Hoc on demand distance vector protocol - протокол маршрутизации по требованию на основе вектора расстояний
AoR, Adress of Record - запись обращения к адресу AoR
AP, Access Point - точка доступа
AS, Autonomous System - автономная система
ATM, Asynchronous Transfer Mode - асинхронный метод передачи
AUC, Authentication Center – центр аутентификации
AUTN, An Authentication token – метка аутентификации
BGP, Border Gateway Protocol) — пограничный шлюзовый протокол
BER, bit error rate - частота ошибочных бит
BPSK, Binary Phase Shift Keyig – бинарная фазовая модуляция
BSC, Base Station Controller – контроллер базовых станций
BSS, Base Transceiver Station – подсистема базовых станций
BTS, Base Transceiver Station - базовая станция
CA, Certification Authority – центр сертификации, удостоверяющий центр.
CDMA, Code Division Multiple Access – множественный доступ с кодовым разделением каналов
CE, Customer Edge router - граничный маршрутизатор клиента
CIC, Circuit Identification Code - код идентификатора канала
COA, Changeover Acknowledgement - подтверждение перевода трафика на резерв
COO, Changeover Order – перевод трафика на резерв
CPE, Cutomer Provider Eguipment - оборудование, усановленное у клиента
CRC, Cyclic redundancy check - циклический избыточный код

CS, Convergence Sublayer - подуровень конвергенции

CSMA/CA, Carrier Sense Multiple Access with Collision Avoidance - множественный доступ с контролем несущей и предотвращением коллизий

DCE, Data Circuit-terminating Equipment - оборудование окончания канала данных

DES, Data Encryption Standard – стандарт шифрования данных

DLCI, Data Link Connection Identifier – идентификатор линий связи данных

DoS, Denial of Service – отказ в обслуживании

DP, Destination Point - пункт назначения

DPC, Destination Point Code - код пункта назначения

DSSS, Direct Sequence Spread Spectrum - расширение спектра методом прямой последовательности

DTE, Data Terminal Equipment - оконечное оборудование данных

DWDM, Dense Wave Division Multiplexing - уплотненное волновое мультиплексирование

EAP, Extensible Authentication Protocol - расширяемый протокол аутентификации

EDGE, Enhanced Data Rates for GSM Evalution – система повышенной скорости передаи данных для развиия GSM

ECB, Electronic Code Book – режим электронного шифроблокнота

EIR, Equipment Identity Register — регистр идентификации оборудования

eNB, evolved Node B — уовершенствованная базовая станция

EPC, Evolved Packet Core – новое поколение базовой сети

ERP, Exterior Routing Protocol - внешний протокол маршрутизации

ETSI, European Telecommunications Standards Institute – Европейский институт стандартизации в области связи

FCS, Frame Check Sequence - контрольная последовательность кадра (КПК)

FDD, Frequency Division Duplex — частотный дуплекс

E-UTRAN, Evolved UTRAN – новое поколение сети радиодоступа UTRAN

FDM, Frequency Division Multiplexing-частотное мультиплексирование

FDMA, Frequency Division Multiple Access – множественный доступ с разделением каналов по частоте

FHSS, Frequency Hopping Spread Spectrum - расширение спектра методом перескока частоты

FEC, Forward Error Correction – прямая коррекция

FEC, Forwarding Equivalency Class – класс эквивалентности по пересылке

FISU, Fill In Signal Unit - заполняющие сигнальные единицы

FR, Frame Relay - ретрансляция кадров

GGSN, GPRS Gateway Service Node – шлюз ядра сети GPRS

GERAN, GSM/EDGE Radio Access Network - система радиодоступа GSM/EDGE, совместимая с UMTS

GMSC, Gateway Mobile Switching Centre – шлюз центра коммутации мобильной связи

GPRS, General Packet Radio Service —система пакетной радиопередача

HDLC, High-level Data Link Control- высокоуровневое управление линией связи

HEC, Header Error Check - контроль ошибок в заголовке

HLR, Home Location Register – домашний регистр местоположения

HSPA, Hight-Speed Packet Access - высокоскоростной пакетный доступ

IAM, Initial Address Message - начальное адресное сообщение

IBSS, Independent Basic Service Set - аналог сети Ad Hoc

IEEE, Institute of Electrical and Electronics Engineers - институт инженеров по электротехнике и электронике

IETF, Internet Engineering Task Force – инженерные группы Интернет, разрабатывающие документы RFC

IMSI, International Mobile Subscriber Identity - международный идентификатор абонента

IN, Intelligent Network – интеллектуальная сеть

INAP, Intelligent Network Application Part - прикладной протокол пользователя интеллектуальной сети

IP, Internet Protocol – Интернет - протокол

IPSec, IP Security – протокол защиты IP

IRP, Interior Routing Protocol - внутренний протокол маршрутизации

ISDN, Integrated Services Digital Network — Цифровая сеть с интеграцией служб

ISUP, Integrated Service User Part - подсистема пользователей сети с интеграцией служб

ITU, International Telecommunication Union – Международный Союз Электросвязи

ITU-R, International Telecommunications Union -Telecommunication Standardizing Sector - Международный Союз Электросвязи - сектор стандартизации в области телекоммуникаций

ITU-T, International Telecommunications Union -Telecommunication Standardizing Sector - Международный Союз Электросвязи - сектор стандартизации в области радиосвязи

IV, Initialization Vector - векторная инициализация

LAI, Location Area Identity – идентификатор области (месторасположения мобильного

абонента)

LAP-B, Link Access Protocol-Balanced - протокол сбалансированного доступа

LCN, Logical Channel Number - логический канальный номер

LDP, Label Distribution Protocol - протокол распределения меток

LER, Label Edge Router – граничный маршрутизатор коммутации по меткам

LIB, Label Information Base - таблица пересылки информации

LSP, Label-Switched Path - коммутируемый по меткам тракт

LSSU, Link Status Signal Unit - сигнальные единицы состояния звена сигнализации

LSR, Label Switching Router – маршрутизатор коммутации по меткам

LTE, Long Term Evolution – система мобильной связи нового поколения

MAC, Medium Access Control - подуровень управления доступом к среде

MAC, Message Authentication Code - код аутентификации сообщения, код аутентичности сообщения

MD5, Message Digest 5 – стандарт хеш-функции

MANET, Mobile Ad Hoc Network - мобильная Ad Hoc сеть

MAP, Mobile Application Part - подсистема мобильных приложений

MBSS, Mesh Basic Service Set - аналог WMN

MCS, Modulation and Coding Scheme – комбинация модуляции и схемы кодирования

Mesh BSS, Mesh Basic Service Set - аналог WMN

MGC, Media Gateway Controller - шлюз сигнализации

MIMO, Multiple Input Multiple Output - множественный вход - множественный выход

MPLS, Multiple Protocol Label Switching – многопротокольная коммутация по меткам

MS, Mobile Station – мобильная станция

MSC, Mobile Switching Centre - Центр коммутации мобильной связи

MSU, Message Signal Unit - значащая сигнальная единица

MTP, Message Transfer Part - подсистема передачи сообщений

NGN, New Generation Network - сети нового поколения

NI, Network Indication - индикатор сети

NNI, Network Node Interface - интерфейс между ATM-коммутаторами

OADM, Optical Add/Drop Multiplexer - оптические мультиплексоры ввода/вывода

OAM, Operation, Administration and Maintenance - администрирование и техническое обслуживание

OFB, Output Feedback - режим группового шифра

OFDM, Orthogonal Frequency Division Multiplexing - мультиплексирование с

ортогональным частотным разделением сигналов

OFDMA, Orthogonal Frequency Division Multiple Access – ортогональный множественный доступ с частотным разделением

OC-N, Optical Carrier level N — оптоволоконная линия связи уровня N

OP, Originating Point - исходящий пункт сигнализации

OPC, Originating Point Code - код исходящего пункта

OSI, Open Systems Interconnect - взаимодействие открытых систем (эталонная модель).

OSPF, Open Shortest Path First — протокол выбор кратчайшего пути первым

P, Provider Router – маршрутизатор провайдера

P-TMSI, Packet Temporary Mobile Subscriber Identity - временной идентификатор мобильного абонента при пакетной коммутации

PDH, Plesiochronous Digital Hierarchy - плезиохронная цифровая иерархия

PDU, Protocol Data Unit – протокол блок данных

PE, Provider Edge Router – граничный маршрутизатор провайдера.

PGP, Pretty Good Privacy — достаточно надежная секретность

PKI, Public Key Infrastructure — инфраструктура систем с открытыми ключами

PRM, Premium Rate — услуга с доплнительной оплатой

PVC, Permanent Virtual Circuit - постоянный виртуальный канал

RFC, Request for Comments – предложения для обсуждения (документы по стандартизации и развитию в Интернет)

RTP, Real-Time Transport - транспортный протокол реального масштаба времени

RSVP, Resource reservation Protocol - протокол резервирования ресурсов

протокол безопасности

QAM, Quadrature Amplitude Modulation — квадратурная амплитудная модуляция

QoS, Quality of Service – качество обслуживания

QPSK, Quadrature Phase Shift Keyig – квадратурная фазовая модуляция

RADIUS, Remote Authentication Dial in User Service - услуга удаленной аутентификации вызывающего пользователя

REJ, reject – кадр «отказ»

RIP, Routing Information Protocol — протокол маршрутной информации

RR, receive ready – кадр «готовность к приему»

RNC, Radio Network Controller – контроллер радиосети

RNR, receive not ready - неготовность к приему

RTP, Real-Time Transport Protocol - протокол реального масштаба времени

RST, Signalling-route-set-test-signal for prohibited destination - тестирование пучка маршрутов для пункта назначения, перенос к котором запрещен

SA, Security Association – защищённая связь

SAE, System Architecture Evolution – новое поколение базовой сети

SAODV, Secure AODV - безопасный протокол AODV

SAR, Segmentation and Reassembly - подуровень сегментации и повторной сборки

SCCP, Signaling Connection Control Part - подсистема управления соединениями сигнализации

SCP, Service Control Point - узел управления услугами

SCMG, SCCP Management - управление подсистемой SCCP

SCRC, SCCP Routing Control - управление маршрутизацией SCCP

SDH,Synchronous Digital Hierarchy - синхронная цифровая иерархия

SEP, Signaling end Point - оконечный пункт сигнализации

SGSN, Serving GPRS Support Node – коммутатор пакетов ядра сети GPRS

SHA-1, Secure Hash Algorithm - безопасный алгоритм хеширования, стандарт хэш-функции

SEP, Signaling End Point - оконечный пункт сигнализации

SI, Service Indication - индикатор вида службы

SIM, Subscriber Identity Module - модуль идентификации абонента

SIP-T, SIP extention for Telepfony - распространение SIP для телефонии

SIP, Session Initiation Protocol - протокол инициирования сеанса

SLA, Service Level Agreement – соглашение об уровне (качестве) обслуживания

SLC, Signaling Link Code- код звена сигнализации

SLS, Signaling Link Selection - поле выбора (селекции) звена сигнализации

SNMP, Simple Network Management Protocol - простой протокол управления сетью

SON, Self-organization - самоорганизующиеся сети

SP, Signaling Point – пункт сигнализации.

SPVC, Switched Permanent Virtual Circuit - коммутируемый постоянный виртуальный канал

SPVC, Soft Permanent Virtual Circuit — программируемый постоянный виртуальный канал

SPR, Signaling Relay Point - пункт сигнализации с функцией переприема сообщений SCCP

SRTP, Secure RTP - протокол безопасности для протокола RTP

SRTSP, Secure RTSP - протокол безопасности для протокола RTSP

SSC, Service Switching Subsystem – подсистема коммуникации

SSL, Security Socket Layer – протокол защищённых сокетов

SSP, Service Switch Point - узел коммутации услуг

SLTM, Signaling link test message - сообщение тестирования звена сигнализации

STP, Signaling Transfer Point – транзитный пункт сигнализации.

STS-N, Synchronous Transport Signal level N — синхронный транспортный сигнал уровня N

STM-N, Synchronous Transport Module level N — синхронный транспортный модуль уровня N

SVC, Switched Virtual Circuit - коммутируемый виртуальный канал

SU, Signaling Unit - сигнальная единица

TA, Telecommunication Actor - участник электросвязи

TAN, Transaction Number - одноразовый пароль

TCAP, Transaction Capability Application Part — прикладная подсистема возможностей транзакций

TCP, Transmission Control Protocol — протокол управлени передачей

TDD, Time Division Duplex - временной дуплекс

TDM, Time Division Multiplexing - временное мультиплексирование

TDMA, Time Division Multiple Access – множественный доступ с разделением каналов по времени;

TFA, Transfer Allowed – разрешение переноса

TFC, Transfer Control – управление переносом (индикация перегрузки)

TFP, Transfer Prohibited – запрещение переноса трафика

TFR, Transfer Restricted – сообщение ограничения переноса трафика

TE, Traffic Engineering - инжиниринг трафика

TKIP, Temporal Key Integrity Protocol — протокол временной целостности ключа

TLS, Transport Layer Security – протокол защиты транспортного уровня

TMN, Telecommunications Management Network - сеть управления электросвязью

TMSI, Temporary Mobile Subscriber Identity - временной идентификатор мобильной станции

UA, User Agent - агент пользователя

UAC, User Agent Client - клиент агента пользователя

UAS, User Agent Client - сервер агента пользователя

UDP, User Data Protocol - протокол пользователей дейтаграмм

UE, User Equipment – оборудование пользователя

UICC, UMTS integrated Circuit Card – съемная плата UMTS

UNI, User-Network Interface - интерфейс между ATM-коммутаторами

UMTS, Universal Mobile Telecommunications System - универсальная система мобильной связи

UPT, Universal Personal Telecommunication – персональная универсальная связь

UPU, User Part Unavailable – подсистема пользователя недоступна модуля идентификации

USIM, UMTS Subscriber Identity Module - модуль идентификации абонента UMTS

UTRAN, Universal Terrestrial Radio Access Network – универсальная наземная сеть радиодоступа (сеть радиодоступа сети UMTS)

VANET, Vehicular Ad Hoc Network- автомобильная беспроводная сеть

VCC, Virtual Circuit Connection – виртуальное канальное соединение

VCI, Virtual Channel Identifier – идентификатор виртуального канала.

VCI, Virtual Channel – идентификаторвиртуального канала

VLR, Visitor Location Register – гостевой регистр местоположения

VoIP, Voice Over IP – передача голосовых данных по сетям IP

VPI, Virtual Path Identifier – идентификатор виртуального пути.

VPI, Virtual Path – виртуальный путь

VPN, Virtual Private Network - виртуальная частная сеть

VRF,VPN Routing and Forwarding table - таблица маршрутизации

WDM, Wave Division Multiplexing - волновое мультиплексирование

WCDMA, Wideband Code Division Multiple Access – широкополосный множественный доступ с кодовым разделением каналов

WEP, Wired Equivalent Privacy – секретность, эквивалентная проводной сети

WBTS, Wideband Base Transceiver Station – широкополосная базовая станция

WiMAX, World Interoperability for Microwave Access — всемирная совместимость при высокочасттно доступе

WMN, Wireless mesh network - беспроводная mesh – сеть (ячеечная сеь)

WSN, Wireless Sensor Network , - беспроводные сенсорные сети

АКД- оборудование окончания канала данных

АМТС - автоматическая междугородная телефонная станция

АС — абонентская станция

АЦП-аналого-цифровой преобразователь

БЛВС - беспроводная локальная вычислительная сеть

БС- базовая станция

ВК — виртуальный канал

ДП — диспетчер программ

ЕСЭ – Единая сеть электросвязи

ЗС – звено сигнализации

ЗнСЕ - значащая сигнальная единица

ИБ – информационная безопасность

ИКМ - импульсно-кодовая модуляция

КВК - коммутируемый виртуальный канал

КК – коммутация каналов

КП – коммутация пакетов.

КПВК - коммутируемый постоянный виртуальный канал

КПК – контрольно-проверочная комбинация, контрольная последовательность кадра

ЛВС- локальная вычислительная сеть

ЛЦК – локальный центр коммутации

МЦК-международный центр комутации

МСЭ-Р, Международный Союз Электросвязи - сектор стандартизации в области радиосвязи

МСЭ-Т, Международный Союз Электросвязи, сектор стандартизации в области телекоммуникаций

НСД — несанкционированный доступ

ОКС№7 – общеканальная сигнализация №7

ООД - оконечное оборудование данных

ПВК- постоянный виртуальный канал

ПК-пакетная коммутация

ПО — программное обеспечение

ССОП- сеть связи общего пользования

ССПС – сотовая сеть подвижной связи

ТфОП – телефонная сеть связи общего пользования.

ТЦК – транзитный центр коммутации.

УАК- узел автоматической коммутации

УК — узел коммутации

ЦАП - цифро-аналоговый преобразователь

ЦКП – центр коммутации пакетов

ЦСИС - цифровая сеть с интеграцией служб

ЦС – центр сертификации

ЭД — электронный документообмен

ЭЦП – электронная цифровая подпись

Литература

Федеральный закон Российской Федерации №126-ФЗ от 7.07.2003 (редакция от 03.12.2011) «О связи».

Москвитин В.Д. От взаимосвязанной сети связи к Единой сети электросвязи России. // Вестник связи. 2003. №8 .С.33-48.

ГОСТ Р 524.48-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.М.: «Стандартинформ», 2006, 15с.

Федеральная Программа «Электронная Россия (2002-2010 г.г.)» // «Электросвязь». 2002. №3. С.25-28.

Матюхин В.Г. Деятельность ФАПСИ по созданию систем электронного документооборота органов государственной власти и реализации ФЦП. //Электронная Россия человеку, обществу, бизнесу: Тез. докл. междун. конф. Москва, 2002. // «Сети и системы связи». 2002. №7/1. С. 9-11.

Коротков А.В. Об электронной торговле в России и роли Федеральной Целевой Программы «Электронная Россия 2002-2010 гг.» и ее развитие. // Электронная Россия человеку, обществу, бизнесу: Тез. докл. междун. конф. Москва, 2002. // Сети и системы связи. №7/1, 2002. С. 14-16.

Денёв М.А., Дыльнов Д.В., Иванов М.А.. Защита информации в банковском и электронном бизнесе. М.: КУДИЦ-ОБРАЗ, 2004. 512с.

Мур М., Притски Т., Риггс К. и др. Телекоммуникации. Спб.: БХВ-Петербург, 2003. 624с.

Столингс В. Основы защиты сетей. Приложения и стандарты. М.: Вильямс, 2002. 324с.

Таненбаум Э. Д. Уэзеролл. Компьютерные сети, 5-е изд. СПБ.: Питер, 2012. 960с.

Мельников Д.А. Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модули.М.: КУДИЦ – ОБРАЗ. 2001. 256с.

Блэк Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы. М.: Мир. 1990. 506с.

Столингс В. Беспроводные линии связи и сети. М.:Вильямс, 2003. 640с

Бельфер Р.А. [и др.]. Проектирование основных функций второго и третьего уровней сетей ПК Х.25. Учебное пособие Инсвязьиздат. М.: 2007. 87с.

Хендерсон Л., Дженкинс Т. Frame Relay. М.: Горячая линия, 2000. 320с. 152с.

ITU-T Recommendation G.1000. Communications Quality of Service: a framework and definitions, 2001.

Файерберг О.И., Шварцман В.О. Качество услуг связи. М.: ИРИАС, 2005. 152с.

Дикер Палтуш Г. Сети АТМ корпорации Cisco. М.: Вильямс, 2004. 880с.

Мартин Джеймс и др. Архитектура и реализация АТМ. М.: Лори, 2000. 214с.

Слепов Н.Н. Синхронные цифровые сети SDH. М.: «ЭКО-ТРЕНДЗ», 1999. 148с.

Гребенщиков А.Ю. Структура и технологии управления сетями связи. – М.: ЭКО-ТРЕНДЗ, 2003. 243с.

Наний О.Е. [и др.]. Перспективные DWDM системы связи со скоростью 20 Тбит/с на соединение. .)» // «Фотон-Экспресс». 2012. №3. С.34-38.

Олифер В.Г., Олифер Н.А. Компьютерные сети, 4-е издание – Спб.: Питер, 2010. 944с.

Столингс В. Беспроводные линии связи и сети. М.: Вильямс, 2003. 640с.

RFC 2574. User-Based Security Model for SNMP, 1999.

ITU-T Recommendation X.805. Security architecture for System providing end-to-end communication, 2003.

ITU-T. Recommendation. X.800. Data communication networks: Open System Interconnection (OSI); Security, Structure and Applications. Security Architecture for Open Systems Interconnection for CCITT Applications, 1991.

Брэгг Р., Родэ-Оусли М., Страссберг К. Безопасность сетей. Полное руководство. М.: ЭКОМ, 2006, 912с.

RFC 2082. RIP-2 MD5 Authentication. 1997.

Столлингс В. Компьютерные сети, протоколы и технологии Интернета. – СПБ.: БХВ-Петербург, 2005. 832 с.

Гольдштейн Ф.Б., Гольдштейн Б.С. Технология и протоколы MPLS. СПБ.: БХВ-Петербург, 2005. 304с.

Оливейн В. Структура и реализация современной технологии MPLS. М.:Вильямс, 2004. 480с.

Беккер П. ISDN. Цифровая сеть с интеграцией служб. Понятия, методы, системы. М.: Радио и связь, 1991. 301с.

ITU-T Recommendation Q.9. Vocabulary of Switching and Signaling Term, 1988

ITU-T Recommendation I.430. Basic User-Network Interface-Layer 1 Specification, 1993.

ITU-T Recommendation Q.920. ISDN User-Network Interface-Date Link Layer- General Aspects, 1993.

ITU-T Recommendation Q.921. ISDN User-Network Interface-Date Link Layer Specification, 1993.

ITU-T Recommendation Q.931. ISDN User-Network Interface Layer 3- Specification for Basic Call Control, 1993.

ITU-T Recommendation Q.702. SPECIFICATION OF SIGNALING SYSTEM No. 7. Signaling data link, 1988.

ITU-T Recommendation Q.703. SPECIFICATION OF SIGNALING SYSTEM No. 7. Message transfer part. Signaling link, 1996.

ITU-T Recommendation Q.704. SPECIFICATION OF SIGNALING SYSTEM No. 7. Message transfer part. Signaling network functions and messages, 1996.

ITU-T Recommendation Q.782. SPECIFICATION OF SIGNALING SYSTEM No. 7. Message transfer part. Signaling system No. 7 test specification – MTP level 3 test specification functions and messages, 2002.

ITU-T Recommendation Q.706. SPECIFICATION OF SIGNALING SYSTEM No. 7. Message transfer part signaling performance, 1993.

ITU-T Recommendation Q.767. SPECIFICATION OF SIGNALING SYSTEM No. 7. Application of the ISDN User Part of CCITT Signaling System No.7 for International ISDN Interconnections,1997.

Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Стек протоколов ОКС7. Подсистема ISUP: Справочник. Спб.: БХВ- Санкт-Петербург. 2003. 220с.

ETSI EN 304 002-1 V1.3.1. Services digital Network (ISDN); Security tools (SET) Procedures;

Digital Subscriber Signaling System № One (DSS1) Protocol; part 1: Protocol Specification, 2001.

ITU-T Recommendation Z.100. Specification and Description Language (SDL), 1993.

G. Chopping and M. Ozdamar. “Security measures in public telecommunications systems”. Second International Conference on Security Communication Systems, London, 1986. C.132-135.

ITU-T Recommendation H.234. Encryption key management and authentication system for audio-visual services, 1998.

ETSI ETS 300 841. Telecommunications Security; Integrated Services digital Network (ISDN); Encryption Key management system for audio-visual services, 1998.

ITU-T Recommendation X.509. Information technology – Open Systems Interconnection. The Directory: Authentication framework (1993 edition – version 2, 1997 edition version 3).

Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи. Учебник для ВУЗов. Спб.: БХВ-Санкт-Петербург. 2011. 400с.

Дэвидсон Д. [и др.]. Основы передачи голосовых данных по сетям IP, 2-изд. М.:Вильямс, 2007. 400с.

Sialem D. [and others]. SIP security. «John Willey & Sons» Ltd, 2009, page. 355.

RFC 3372. Sesion Initiation Protocol for Telephones (SIP-T): Context and Architectures.

Гольдштейн Б.С., Зарубин А.А., Саморезов В.В. Протокол SIP. Справочник. Спб.: БХВ-Санкт-Петербург. 2005. 400с.

RFC 3261. SIP: Sesion Initiation Protocol, 2002.

RFC 2543. SIP: Sesion Initiation Protocol, 1999.

RFC 2617. HTTP Authentication: Basic and Digest Access Authenti, 1999.

RFC 4474. Enhancements for Audenticated Identity Management in the Session Initiation Protocol SIP, 2009.

Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и связь, 2001, 501с.

Интеллектуальные сети связи. / Лихтциндер Б.Я. [и др.] М.: ЭКО-ТРЕНДЗ, 2000, 205с.

Росляков А.В. Общеканальная сисема сигнализации. М.: ЭКО-ТРЕНДЗ, 2002, 230с.

ETSI ETR 083. Universal Personal Telecommunication (UPT); General UPT security architecture, 1993.

ETSI ETR 320. Security Techniques Advisory Group (STAG), Security requirements capture, 1996.

ETSI ETR 232. Security Techniques Advisory Group (STAGE), Glossary of security terminology, 1995.

Бельфер Р.А. Анализ систем связи в аспекте проектирования информационной безопасности // Электросвязь. 2004. №3, С.22-24.

Шиллер Й. Мобильные коммуникации. М.: Вильямс, 2002, 384с.

Ратынский М.В. Основы сотовой связи.М.: Радио и связь, 2-е издание, 2000, 248с.

Веселовский Кшиштоф. Системы подвижной радиосвязи. – М.: Горячая линия – Телеком, 2006, 536с.

Защита информации в системах мобильной связи. / Чекалин А.А. [и др.]. Учебное пособие, - 2-е издание. М.: Горячая линия, 2005, 171с.

Драйберг Ли, Хьюит В. Система сигнализации №7 (SS7/ОКС7), протоколы, структура и применение. М.: Вильямс, 2006, 752с.

Бельфер Р.А., Горшков Ю.Г. Система сигнализации ОКС-7. Требования к QoS и организация программного обеспечения сетевого уровня. Учебное пособие. М.: Информсвязьиздат, 2007, 87с.

Бельфер Р.А., Горшков Ю.Г., Даннави М.Н. Последствия нарушений маршрутизации общеканальной сигнализации на функционирование сетей связи общего пользования // Вестник МГТУ им. Н.Э. Баумана сер. «Приборостроение». 2009, №3, С.90-94.

Бельфер Р.А., Горшков Ю.Г., Даннави М.Н. Архитектура сетевой безопасности ОКС-7 // Электросвязь, 2004, №4, С.12-15.

Горшков Ю.Г., Бельфер Р.А. Анализ риска информационной безопасности сетей GSM при выполнении функций защиты приватности // Электросвязь, 2012, №3, С.26-28.

Бельфер Р.А., Морозов А.М. Информационная безопасность сети связи для соединений абонентов ТфОП/ISDN через протокол SIP-T // Электросвязь, 2012, №3, С.22-25.

Gerhard Rufa. Developments in Telecommunications. With a Focus on SS7 Network Reliability, Springer, 2008, page.283.

Максим М., Поллино Д. Безопасность беспроводных сетей. М.: Компания Ай Ти; ДМК Пресс, 2004, 288с.

Сети следующего поколения NGN. / Росляков А.В. [и др.]. М.: Эко-Трендз, 2008, 424с.

Бельфер Р.А., Акулов А.П. Безопасность мобильных систем связи 3G // Вестник связи. 2001. №12, С.58-60.

Bannister J.[and others]. Convergence Technologies for 3G Networks. IP, UMTS, EGPRS and ATM. «John Wiley & Sons, Ltd», 2004., page.650.

Кааранен Х. [и др.]. Сети UMTS. Архитектура, мобильность, сервисы. М.: Техносфера, 2007, 464с.

Niemi V., Nyberg K. UMTS Security «John Wiley & Sons, Ltd», 2003, page.273.

3GPP TS 121 133 V3.2.0. Universal Mobile Telecommunications Systems (UMTS); 3G Security; Security Threats and Requirements. 2001.

Бельфер Р.А. Способы классификации угроз безопасности сетей связи ВСС России (на примере ISDN, IN, UMTS) и возможные методы их количественной оценки // Электросвязь. 2002, №7, С. 14-18.

Вишневский В.М., Портной С.Л., Шахнович И.В. Энциклопедия WiMAX. Путь к 4G. М.: Техносфера, 2009, 472с.

Дэвис Д. Создание защищенных беспроводных сетей 802.11 в Microsoft Windows. Справочник профессионала. М.: ЭКОМ, 2006, 400с.

Молчанов Д.А. Самоорганизующиеся сети и проблемы их построения. Электросвязь, 2006, №6, С.20-22.

Немировский М.С. Беспроводные технологии от последней мили до последнего дюйма. М.:Эко-Трендз, 2009, 400с.

David Tung Chongs Wong [and others]. Wireless Broadband Networks, «John Willey & Sons» Ltd,

2009, page. 527.

Ping Yi [and others]. A Survey on Security in Wireless Mesh Networks, IETE Technical Review, v.27, 2010, №1, PP.6-14

S. Glass, M. Portmann, V. Muthukkumarasamy. Securing Route and Path Integrity I Multihop Wireless Networks. PP.25-29. Security of Self-Organizing Networks. MANET, WSN, WMN, VANET. CRC Press, 2011, page.595.

Rong-Hong Jan, Huel-Ru Tseng, Wuu Yang. Wireless LAN Security. P.399-418, Wireless Ad Hoc Netwoking. Auerbach Publications, 2007, page.640.
Floriano De Rango, Andrea Malfitano and Salvatore Marano. 111-144 p. WiMAX Cross-Layer End-to-End QoS Architecture: The Milestone of WiMAX SECURITY AND QUALITY OF SERVIC AN END-TO-END PERSPECTIVE. «John Willey & Sons» Ltd, 2010, page.425.
Bogdanoski M [and others]. IEEE 802.16 Security Issues // A servey. 16th Telecommunications forum TELFOR:Serbia, Belgrad, 2008. P. 199-202.

Тихвинский В.О. Мобильный мир: успехи и угрозы. Итоги MVC-2012. //Электросвязь, 2012, №4, С.18-19.

Тихвинский В.О., Терентьев С.В., Юрчук А.Б. Сети мобильной связи LTE: технологии и архитектура. М.: Эко-Трендз, 2010, 284с.

Голышко А.В. Самая полная информация о том, что на самом деле дает LTE //Вестник связи, 2011, №6, С.44.

Нетес В.А. Скорости широкополосного доступа //Электросвязь 2011, №10, С. 47-49.

Совместимость – новое свойство сети в новых рынках //Электросвязь 2011, №7, С. 17.

Farood Anjum, Petros Mouchtaris. Security for Wireless Ad Hoc Networks. «John Wiley & Sons» Ltd, 2007, page.247.

Erdal Cayirici, Chunming Rong. Security in Wireless Ad Hoc and Sensor Networks. «John Willey & Sons» Ltd, 2009, page.257.

Молчанов Д.А., Кучерявый Е.А. Приложения беспроводных сенсорных сетей // Электросвязь. 2009. №1, С.20-22.

Ian F. Akyildiz, Xudong Wang. Wireless Mesh Network, «John Wiley & Sons» Ltd, 2009, page.327.

Anna Hack. Wireless Sensor Network Designs, «John Wiley & Sons» Ltd, 2003, page.391.

Manel Guerrero Zapata. Secure Routing in Wireless Mesh Networks. PP.171-194. Security Routing in Wireless Mesh Networks. CRC Press, 2011, page.536.

Vibrant Go hale, S.K. Gosh, Armband Gupta. Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks. PP.196-217. Security of Self-Organizing Networks. MANET, WSN, WMN, VANET. CRC Press, 2011, page.595.

Е.А. Кучерявый, А.В. Винкель, С.В. Ярцев. Особенности развития и текущие проблемы автомобильных беспроводных сетей VANET. // Электросвязь. 2009. №1, С.24-28.

Vicas Singh Yadav, Sudip Misra, Mozaffar Afaque. Security in Vehicular Ad Hoc Networks. PP.228-249. Security of Self-Organizing Networks. MANET, WSN, WMN, VANET. CRC Press, 2011, page.595.

ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.

ETSI ETR 332. Security Technicques Advisory Group (STAG), Security requirements capture,

1996.

И. Ченнинг. Борьба с мошенничеством продолжается. Мобильные телекоммуникации, 2001, №6, С.23-27.

ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных. 28с.

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».