



Александр Филимонов

Протоколы Интернета

- ЛВС и удаленный доступ
- Внутренняя и внешняя маршрутизация
- Управление компонентами сети
- Формирование и интеграция потокового трафика



МАСТЕР СИСТЕМ

Александр Филимонов

Протоколы Интернета

Санкт-Петербург

«БХВ-Петербург»

2003

УДК 681.3.06
ББК 32.973.202
Ф53

Филимонов А. Ю.

Ф53 Протоколы Интернета. — СПб.: БХВ-Петербург, 2003. — 528 с.: ил.
ISBN 5-94157-247-6

В книге подробно рассматриваются основные принципы построения и особенности применения наиболее популярных протоколов, используемых в современных сетях Интернета, а также направления их дальнейшего развития. Большое внимание уделено протоколам маршрутизации, управления компонентами сети и транспортным протоколам глобальной сети. Освещаются перспективные протоколы и технологии, предназначенные для обеспечения информационной безопасности современных вычислительных сетей, формирования и интеграции в них голосового и видеотрафика. Значительная часть книги посвящена рассмотрению протоколов таких популярных интернет-служб, как e-mail, WWW и др. Полнота представленного материала, подкрепленного практическими примерами, обеспечивает глубокое понимание принципов организации информационно-вычислительных сетей и успешную реализацию их на практике.

*Для администраторов сетей,
сотрудников IT-отделов предприятий и студентов*

УДК 681.3.06
ББК 32.973.202

Группа подготовки издания:

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Анна Кузьмина</i>
Редактор	<i>Юрий Рожко</i>
Компьютерная верстка	<i>Татьяны Олоновой</i>
Корректор	<i>Виктория Голуб</i>
Оформление серии	<i>Via Design</i>
Дизайн обложки	<i>Игоря Цырульников</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 22.11.02.

Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 42,57.

Тираж 4000 экз. Заказ №

"БХВ-Петербург", 198005, Санкт-Петербург, Измайловский пр., 29.

Гигиеническое заключение на продукцию, товар № 77.99.02.953 Д.001537.03.02
от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов
в Академической типографии "Наука" РАН
199034, Санкт-Петербург, 9 линия, 12.

ISBN 5-94157-247-6

© Филимонов А. Ю., 2002

© Оформление, издательство "БХВ-Петербург", 2002

Содержание

Глава 1. Обзор протоколов Интернета	1
Рождение TCP/IP. История создания Интернета	1
Иерархическая система информационного взаимодействия	3
Уровень приложения	8
Уровень представления	8
Уровень сессии	8
Транспортный уровень	8
Сетевой уровень	9
Канальный уровень	9
Физический уровень	10
Взаимодействие на сетевом уровне Интернета	10
Адресация в IP-сетях	12
Сетевой IP-адрес (классы, структура)	12
Специфические адреса Интернета	14
Взаимодействие на сетевом уровне Интернета	19
Структура дейтаграммы IP	20
Формат заголовка дейтаграммы IP	20
Фрагментация и дефрагментация IP-дейтаграмм	22
Обзор протоколов, применяемых в Интернете	24
Прикладные сервисы TCP/IP	26
Глава 2. Протоколы канального уровня	33
Протокол SLIP	34
Протокол PPP	36
Служебный протокол LCP	40
Сообщение Configure-Request	41
Сообщение Configure-Ack	41
Сообщение Configure-Nak	42
Сообщение Configure-Reject	42

Сообщения Terminate-Request и Terminate-Ack.....	43
Сообщение Code-Reject	43
Сообщение Protocol-Reject	43
Сообщения Echo-Reply и Echo-Request.....	44
Сообщение Discard-Request.....	44
Протоколы аутентификации PAP и CHAP	44
Многоканальный протокол PPP	45
Организация связки каналов MLP.....	46
Структура фрагментов MLP.....	47
Обнаружение потери фрагмента MLP	49
Протоколы локальных вычислительных сетей	50
Сети CSMA/CD (Ethernet)	50
Сети с маркерным доступом	53
Сети Token Ring.....	54
Сети FDDI.....	57
Протокол ARP	58
ARP cache	62
Прогу ARP	62
Утилита ARP MS Windows и способы ее использования	62
Глава 3. Протоколы управления и контроля сетевых компонентов.....	65
Классы и задачи служебных протоколов	65
Протоколы мониторинга состояния сети	65
Протоколы управления компонентами сети	66
Протокол ICMP	66
Структура сообщения ICMP.....	67
Структура заголовка сообщений ICMP.....	68
Сообщение Destination Unreachable	69
Сообщение Time Exceeded	70
Сообщение Parameter Problem.....	71
Сообщение Source Quench	72
Сообщение Redirect	73
Сообщения Echo Request/Reply.....	75
Атаки с использованием ICMP Echo Request/Reply	76
Способы защиты от атак с использованием	
ICMP Echo Request/Reply.....	78
Утилита PING	79
Утилита TRACEROUTE.....	80
Утилита PATHPING.....	81
Сообщения Timestamp Request/Reply	82
Сообщения Address Mask Request/Reply	83
Протоколы RARP и DHCP.....	84
Протокол RARP.....	84
Организация RARP-взаимодействия компонентов сети	85

RARP-сервер	85
Протокол DHCP	87
Механизм динамического назначения адресов	88
Реализация протокола DHCP	89
Протоколы динамического резервирования	92
Назначение протокола HSRP	92
Состояния события и таймеры маршрутизаторов HSRP	94
Формат и типы пакетов HSRP	95
Взаимодействие HSRP с протоколами ARP и ICMP	96
Протокол VRRP	97
Протокол SNMP	98
Принципы построения системы управления сетью	99
Глобальное дерево имен	101
Взаимодействие компонентов протокола SNMP	104
Протокол RPC	107
Принципы построения протокола	108
Структуры сообщений протокола	110
Протокол TELNET	111
Принципы построения	112
Сетевые виртуальные терминалы — NVT	113
Описание протокола	116
TELNET — универсальный клиент	117

Глава 4. Маршрутизация в сетях TCP/IP 123

Принцип "Hop-by-Hop"	123
Статическое и динамическое определение маршрута	124
Домены маршрутизации и автономные системы	129
Протоколы внешней и внутренней маршрутизации	130
Протоколы RIP и IGRP	131
Формирование таблицы маршрутизации в алгоритмах "Distance-Vector"	131
Возникновение циклических маршрутов	133
Процедуры Split Horizon и Poison Reverse	135
Управляемое обновление маршрутов (Triggered Update)	137
Особенности алгоритма RIP II	138
Таймеры	138
Сообщения протокола RIP	139
Маршрутизация для внеклассовых сетей	142
Установление подлинности источника маршрутной информации	142
Протокол IGRP	143
Примеры практического применения протоколов RIP II и IGRP	145

Протокол маршрутизации OSPF.....	146
Формирование маршрутных таблиц алгоритмами "Link-State".....	149
Иерархия областей и роли маршрутизаторов OSPF.....	150
Представление информации о состоянии компонентов сети (LSA)	151
Построение и обслуживание топологической базы маршрутов протокола OSPF.....	153
Сообщения протокола OSPF	155
Пример практического применения алгоритма протокола OSPF.....	161
Протокол маршрутизации EIGRP.....	162
Особенности гибридных протоколов маршрутизации	163
Алгоритм DUAL	164
Обеспечение быстрой сходимости и совместимости протоколов EIGRP и IGRP	168
Отношения между маршрутизаторами. Назначение и типы сообщений протокола EIGRP	170
Пример практического применения алгоритма протокола EIGRP	172
Протокол маршрутизации EGP.....	173
Назначение и особенности протоколов внешней маршрутизации	175
Взаимодействие маршрутизаторов протокола EGP, назначение и типы сообщений.....	177
Ограничения и недостатки протокола EGP.....	184
Протокол маршрутизации BGP.....	184
Способы распространения маршрутной информации протокола BGP	185
Атрибуты маршрутов.....	187
Понятие и способы реализации политики маршрутизации.....	190
Процедура определения оптимального маршрута	191
Особенности протокола BGP.....	192
Типы и форматы сообщений протокола BGP	194
Пример практического использования алгоритма протокола BGP	198

Глава 5. Транспортные протоколы Интернета201

Протокол UDP.....	202
Протокол TCP	205
Способы обеспечения надежного информационного обмена.....	205
Взаимодействие с приложениями	206
Мультиплексирование информационных потоков, механизм гнезд (sockets)	208
Установление соединения и передача данных	209

Обеспечение гарантированной доставки данных.....	210
Управление темпом информационного обмена	213
Формат сегмента протокола TCP	214
Особенности практической реализации протокола TCP	215
Протокол RTP	217
Принципы построения протокола RTP.....	218
Сообщения протокола RTP	224
Сообщения протокола RTCP.....	226
Сообщения Sender Report.....	227
Сообщения Receiver Report	229
Сообщения Source Description	230
Сообщения BYE.....	231

Глава 6. Протоколы группового взаимодействия в сети Интернет233

Особенности взаимодействия с использованием Multicast-адресов.....	233
Диапазоны групповых адресов TCP/IP	235
Передача группового трафика на канальном уровне.....	238
Определение состава группы	239
Маршрутизация и доставка группового трафика	240
Протокол IGMP	241
Формат сообщения протокола IGMP	244
Особенности использования и обеспечение с овместимости протокола IGMP версий v1 и v2	246
Дальнейшее развитие протокола IGMP	248
Практическая реализация протокола IGMP в современных сетях.....	248
Протокол CGMP (Cisco Systems)	250
Прослушивание сообщений протокола IGMP коммутаторами ЛВС	251
Протоколы групповой маршрутизации.....	254
Режимы доставки группового трафика.....	254
Протокол DVMRP.....	258
Принцип построения маршрута протоколом DVMRP	258
Сообщения протокола DVMRP.....	261
Протокол PIM.....	262
Особенности использования PIM в режиме DENSE.....	263
Режим SPARSE протокола PIM.....	264

Глава 7. Интеграция разнородного трафика в сетях TCP/IP.....267

Принципы построения мультимедийных компонентов сети Интернет ...	270
Терминальные устройства H.323	272
Компоненты и функции терминальных устройств H.323	273
Компоненты и функции шлюза H.323.....	278
Компоненты и функции привратника H.323.....	279

Протокол RSVP	281
Механизмы управления трафиком протокола RSVP	282
Формы и методы резервирования ресурсов	284
Стиль Wildcard-Filter (WF)	285
Стиль Fixed-Filter (FF)	286
Стиль Shared Explicit (SE)	287
Сообщения протокола RSVP	288
Сообщения Reservation-Request	288
Сообщения Path	288
Сообщения Error	288
Сообщения Confirmation	289
Сообщения Teardown	289
Формат сообщений протокола RSVP	289
Принципы построения и компоненты сетей VoIP	291
Компоненты и алгоритмы систем VoIP	292
Терминальные устройства VoIP	292
Принципы построения и компоненты шлюзов VoIP	295
Функции привратника VoIP	297
Пример практического применения технологии VoIP	297

Глава 8. Обеспечение информационной безопасности в сетях TCP/IP299

Комплекс протоколов IPsec	300
Схемы защиты информации	300
Соединения безопасности IPsec	303
Состав комплекса протоколов IPsec	304
Протокол заголовка аутентификации AH	304
Структура заголовка аутентификации протокола AH	304
Размещение заголовка аутентификации	305
Вычисление контрольного значения заголовка — ICV	306
Протокол защиты полезной нагрузки ESP	307
Формат блока данных протокола ESP	308
Размещение блока данных протокола ESP в IP-пакете	309
Процедура обработки порядковых номеров пакетов	310
Структура систем обеспечения безопасности IPsec	311
Процедуры аутентификации	311
Базы данных систем безопасности	312
Применение технологии MPLS в сети Интернет	315
Основные понятия и компоненты MPLS	316
Основные принципы построения MPLS-систем	318
Структура метки MPLS	319
Стеки меток MPLS	320
Принципы построения виртуальных частных сетей	321
Типы виртуальных частных сетей	322

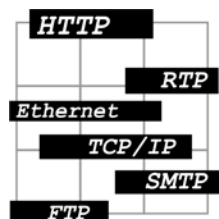
Технологии виртуальных частных сетей.....	324
Виртуальные сети на основе технологий IPsec	324
Виртуальные сети на основе технологии MPLS.....	326
Глава 9. Система доменов и распределенная база данных DNS	329
История создания DNS.....	331
Решения DNS.....	331
Состав и основные компоненты DNS	332
Пространство имен домена и записи базы данных.....	336
Спецификация.....	336
Записи базы данных.....	337
Текстовое представление данных.....	342
Имена и псевдонимы.....	344
Запросы. Стандартные и инверсные запросы	344
Серверы имен.....	348
Понятие зоны. Деление DNS-пространства на зоны	348
Механизмы и алгоритмы обслуживания запросов.....	350
Инсталляция и перемещение зон	353
Программы разрешения имен.....	354
Интерфейс разрешения имен	354
Функциональность.....	355
Пример построения и инсталляции DNS.....	359
Примеры построения запросов и ответов серверов имен.....	362
Примеры работы программы разрешения имен	366
Утилита NSLOOKUP.....	368
Глава 10. Протоколы электронной почты — SMTP, POP3, IMAP4	371
Протокол SMTP.....	371
Формат почтовых сообщений MIME	372
Взаимодействие компонентов SMTP.....	380
Организация информационного обмена	381
Ретрансляция сообщений.....	386
Примеры выполнения транзакций протокола SMTP	388
Использование протокола SMTP для передачи 8-битных данных	390
Взаимодействие SMTP с протоколом TCP	392
Протокол POP3	393
Основные принципы протокола POP3.....	393
Организация информационного обмена.....	395
Пример использования протокола POP3	399
Протокол IMAP4.....	400
Основные принципы протокола IMAP4	401
Атрибуты сообщений IMAP-системы.....	402
Основные команды протокола IMAP4	403
Пример взаимодействия IMAP4-клиента с сервером	408

Глава 11. Протокол передачи новостей — NNTP	411
Система новостей UseNet	411
Способы тиражирования сообщений	412
Серверы новостей.....	413
Формат статей и сообщений системы UseNet	414
Управляющие сообщения.....	418
Модели передачи статей.....	420
Протокол NNTP, описание команд	422
Пример передачи статьи по протоколу NNTP	426
Глава 12. Протокол HTTP	429
Сервисы сети WWW	429
Принципы построения HTTP-соединения.....	432
Описание протокола HTTP	434
Организация запроса протокола HTTP.....	435
Структура ответа протокола HTTP	441
Механизмы аутентификации	443
Взаимодействие протокола HTTP и CGI-сервиса.....	445
Расширение возможностей протокола HTTP	448
Глава 13. Протоколы передачи файлов	451
Основные принципы протокола FTP.....	451
Описание команд протокола.....	455
Сценарий работы протокола FTP.....	457
Протоколы TFTP и SFTP	458
Утилита FTP	461
Глава 14. Сетевая файловая система — NFS	465
Принципы построения протокола.....	466
Файловая система.....	466
Механизм аутентификации.....	467
Описание протокола.....	468
Глава 15. Направления дальнейшего развития протокола IP	471
Предпосылки и направления модернизации TCP/IP	471
Технология вложенных заголовков.....	473
Основной заголовок протокола IPv6	475
Сетевые адреса протокола IPv6.....	478
Категории сетевых адресов	478
Формы представления сетевых адресов протокола IPv6	479
Специальные сетевые адреса протокола IPv6.....	480
Заголовки расширения протокола IPv6	481
Заголовок Hop-by-Hop Options.....	481

Заголовок маршрутизации Routing Header.....	483
Заголовок фрагментации Fragment Header.....	484
Заголовок Destination Options Header	485
Заголовки информационной безопасности протокола IPv6	486
Грандиозное переселение.....	486
Глоссарий	489
Предметный Указатель	507

Глава 1

Обзор протоколов Интернета



Рождение TCP/IP. История создания Интернета

В научном и техническом мире существует мнение, что чаще всего перспективные и передовые технологии рождаются при изобретении нового оружия или средств защиты от него. Это объясняется тем, что система, предназначенная для работы в экстремальных условиях, надежно и устойчиво функционирует в мирное время. Именно так и случилось с Интернетом и протоколами семейства TCP/IP (Transmission Control Protocol/Internet Protocol).

Идея создания Интернета была предложена RAND Corporation (США) в связи с необходимостью построения коммуникационной отказоустойчивой сети, которая могла бы функционировать даже в том случае, если большая часть ее узлов вышла из строя, например, в случае ядерной войны. Решение состояло в том, чтобы создать сеть, где информационные пакеты могли бы передаваться от одного узла к другому без какого-либо централизованного контроля. В случае, если бы основная часть сети не работала, пакеты самостоятельно передвигались бы по доступным узлам до тех пор, пока не попали бы в точку своего назначения. Кроме того, сеть должна была быть достаточно устойчива к возможным ошибкам при передаче пакетов, т. е. обладать механизмом контроля пакетов и обеспечивать контроль доставляемой информации. Хотя проект был по своей сути военным, к его разработке привлекались научные институты и университеты.

В начале 70-х годов созданием такой сети занялось Агентство Передовых Проектов Национальной Безопасности США (United States Defense Advanced Research Project Agency — DARPA). Точнее, история Интернета началась в 1969 году, когда в Калифорнийском университете был установлен первый узел сети, получивший название ARPAnet (по имени компании, финансировавшей проект), и были созданы основы для построения сети с коммутируемыми пакетами. К началу 1971 года ARPAnet насчитывала уже около 20 узлов, и более 30 университетов получили возможность подключения к сети в рамках проекта.

К середине 70-х были предприняты попытки объединения различных пакетных сетей. В начале 80-х к ARPAnet были подключены первые локальные

сети, и для использования в построенной сети (в дальнейшем именуемой Интернетом) был выбран, адаптирован и затем повсеместно принят для работы набор протоколов Transmission Control Protocol/Internet Protocol (TCP/IP). Он сменил более ранний протокол NCP (Network Communication Protocol). TCP/IP вполне удовлетворял всем тем требованиям, которые на него возлагались. По сути дела, это и послужило началом широкого распространения TCP/IP. Что из этого вышло — мы можем судить по той скорости, с которой внедряется в нашу жизнь Интернет.

Существует много причин, почему протоколы семейства TCP/IP были выбраны за основу в сети Интернет. Это, прежде всего, возможность работать с этими протоколами как в локальных LAN (Local Area Network), так и в глобальных WAN (Wide Area Network) сетях, способность протоколов управлять большим количеством стационарных и мобильных пользователей, удобство для использования частными лицами или организациями, желающими подключиться прямо к Интернету или через фирмы, предоставляющие этот сервис. Протоколы Интернета обеспечивают высокий уровень взаимодействия между совершенно различными операционными системами, предоставляют средства для разработки на их основе приложений, использующих современный программный интерфейс. Но главную роль, безусловно, сыграло провидение разработчиков ARPAnet, когда они выбирали этот почти никому не известный протокол для построения своей тогда еще крохотной сети.

В 1986 году на базе существующей опорной сети ARPAnet, которая обладала производительностью 56 Кбит/с и объединяла шесть суперкомпьютерных центров США, было начато строительство новой сети. Решение о модернизации было принято вследствие загруженности существующей инфраструктуры. Заказ на проведение проекта получил консорциум Merit, MCI и IBM. При реализации этого проекта самой сложной проблемой был поиск специалистов, знающих технологию сетей и, в частности, TCP/IP. Однако уже через 8 месяцев система на базе каналов T1 (1,54 Мбит/с) была сдана в эксплуатацию. Она состояла из 13 коммутационных узлов, каждый из которых составляли 9 параллельно работающих компьютеров IBM, работающих под управлением Berkeley UNIX и соединенных локальной сетью. Узлы занимались маршрутизацией пакетов и сбором сетевой информации. Причем каждый был построен таким образом, что при выходе его из строя выполняемые им функции принимали на себя оставшиеся узлы.

Дальнейшее развитие Интернета шло подобно снежному кому. Ядро обрастало все большим и большим количеством узлов, соединений и подключенных сетей. И уже в 1989 году загрузка опорных линий достигла предельных значений. Поэтому в 1991 году была выполнена модернизация и сеть была переведена на линии T3 (45 Мбит/с), причем коммутационные компьютеры были заменены на ЭВМ IBM RS/6000. К тому времени сеть уже насчитывала 16 узлов и более 3500 подключенных сетей.

В настоящее время скорости информационного обмена сети Интернет и темпы ее роста продолжают увеличиваться.

Иерархическая система информационного взаимодействия

Информационное взаимодействие в сети Интернет строится в соответствии с правилами и требованиями общего международного стандарта ISO 7498 (ISO — International Organization for Standardization).

Этот стандарт имеет тройной заголовок "Информационно-вычислительные системы — Взаимодействие открытых систем — Эталонная модель". Обычно его называют короче — "Эталонная модель взаимодействия открытых систем". Публикация этого стандарта в 1983 году подвела итог многолетней работы многих известных телекоммуникационных компаний и стандартизирующих организаций.

Основной идеей, которая положена в основу этого документа, является разбиение процесса информационного взаимодействия между системами на уровни с четко разграниченными функциями.

Идея такого разбиения не была революционной. Можно вспомнить, что слоистую архитектуру имели информационные взаимодействия в сетях SNA (Systems Network Architecture) и DNA (Digital Network Architecture).

В качестве прообраза модели взаимодействия OSI (Open System Interconnection) была использована структура, предложенная ANSI (American National Standards Institute). Основные работы по созданию текста документа были выполнены CCITT (Consultative Committee for International Telegraphy), а итоговый документ появился в виде стандарта ISO. Статус стандарта ISO важен для данного документа, поскольку ISO 7498 является стандартом стандартов в области телекоммуникаций.

Преимущества слоистой организации взаимодействия заключаются в том, что она обеспечивает независимую разработку уровней стандартов, модульность аппаратуры и программного обеспечения информационно-вычислительных систем и способствует тем самым техническому прогрессу в данной области.

При использовании многоуровневой модели проблема перемещения информации между узлами сети разбивается на более мелкие и, следовательно, более легко разрешимые проблемы.

Многоуровневая модель четко описывает, каким образом информация продвигается путь через среду сети от одной прикладной программы, к примеру, обработки таблиц, до иной прикладной программы обработки тех же таблиц, находящейся на другом компьютере сети.

Предположим, например, что система А, изображенная на рис. 1.1, имеет информацию для отправки в систему В. Прикладная программа системы А начинает взаимодействовать с уровнем 4 системы А (верхний уровень), который, в свою очередь, начинает взаимодействовать с уровнем 3 системы

А, и т. д. — до уровня 1 системы А. Задача уровня 1 — отдавать, а потом забирать информацию из физической среды сети.

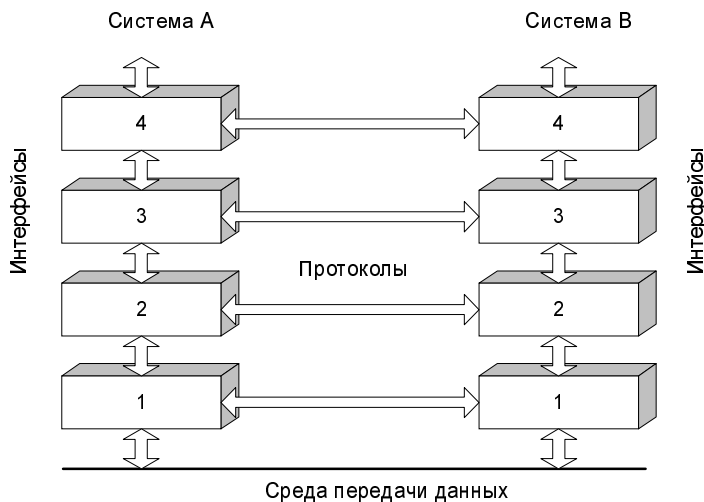


Рис. 1.1. Организация информационного взаимодействия двух систем

Примечание

Поскольку информация, которая должна быть отослана, проходит вниз через уровни системы, по мере этого продвижения она становится все меньше похожей на человеческий язык и все больше похожей на ту информацию, которую понимают компьютеры, а именно "единицы" и "нули".

После того как информация проходит через физическую среду сети и поступает в систему В, она последовательно обрабатывается на каждом уровне системы В в обратном порядке — сначала на уровне 1, затем на уровне 2 и т. д., пока, наконец, не достигнет прикладной программы системы В.

Многоуровневая модель не предполагает наличия непосредственной связи между одноименными уровнями взаимодействующих систем. Следовательно, каждый уровень системы А должен полагаться на услуги, предоставляемые ему смежными уровнями системы А, чтобы помочь осуществить связь с соответствующим уровнем системы В. Предположим, что уровень 4 системы А должен связаться с уровнем 4 системы В. Для того чтобы выполнить эту задачу, уровень 4 системы А должен воспользоваться услугами уровня 3 системы А, тогда уровень 4 будет называться "пользователем услуг", а уровень 3 — "источником услуг".

Информация по оказываемым услугам передается между уровнями в специальном информационном блоке, который называется *заголовком*. Заголовок обычно предшествует передаваемой прикладной информации.

Предположим, что система А хочет отправить в систему В какой-либо текст, называемый "данные" или "информация". Этот текст передается из прикладной программы системы А в верхний уровень этой системы. Прикладной уровень системы А должен передать определенную информацию в прикладной уровень системы В, поэтому он помещает управляющую информацию своего уровня в виде заголовка перед фактическим текстом, который должен быть передан. Построенный таким образом информационный блок передается в уровень 3 системы А, который может предварить его своей собственной управляющей информацией, и т. д.

Размеры сообщения увеличиваются по мере того, как оно проходит вниз через уровни до тех пор, пока не достигнет сети, где оригинальный текст и вся связанная с ним управляющая информация перемещаются в систему В и поглощаются уровнем 1 системы В. Уровень 1 системы В отделяет от поступившей информации и обрабатывает заголовок уровня 1, после чего он определяет, как обрабатывать поступивший информационный блок. Слегка уменьшенный в размерах информационный блок передается в уровень 2, который отделяет заголовок этого же уровня, анализирует его, чтобы узнать о действиях, которые он должен выполнить и т. д. Когда информационный блок наконец доходит до прикладной программы системы В, он должен содержать только оригинальный текст.

Структура заголовка и собственно данных относительно и зависит от уровня, который в данный момент анализирует информационный блок. Например, на уровне 2 информационный блок состоит из заголовка этого же уровня и следующих за ним данных. Однако данные уровня 2 могут содержать заголовки уровней 3 и 4. Кроме того, заголовок уровня 2 является просто данными для уровня 1. Помимо заголовка на каждом уровне системы информационный блок завершается соответствующей контрольной суммой КонтСум. Эта концепция иллюстрируется на рис. 1.2.

Данная модель напоминает собой вложенные друг в друга матрешки. Самая маленькая из них — это и есть пользовательские данные, а все остальные служат для доставки данных в точку назначения.

Иными словами, в результате работы этого механизма каждый пакет более высокого уровня вкладывается в "конверт" протокола нижнего уровня. Здесь уместно провести аналогию с обычными почтовыми отправлениями. Так, например, если вы пишете обычное письмо и вкладываете его в конверт с адресом, то текст письма будет информационным сообщением, которое вы хотите отправить, а конверт — заголовком "почтового" протокола. На почте ваше письмо перекладывают в мешок (протокол более низкого уровня) с письмами того же или близкого назначения и т. п. Электронные протоколы работают по той же схеме, только доставку и целостность обычных писем обеспечивает добросовестность служащих отделений связи, а электронным протоколам приходится следить за этим самостоятельно.

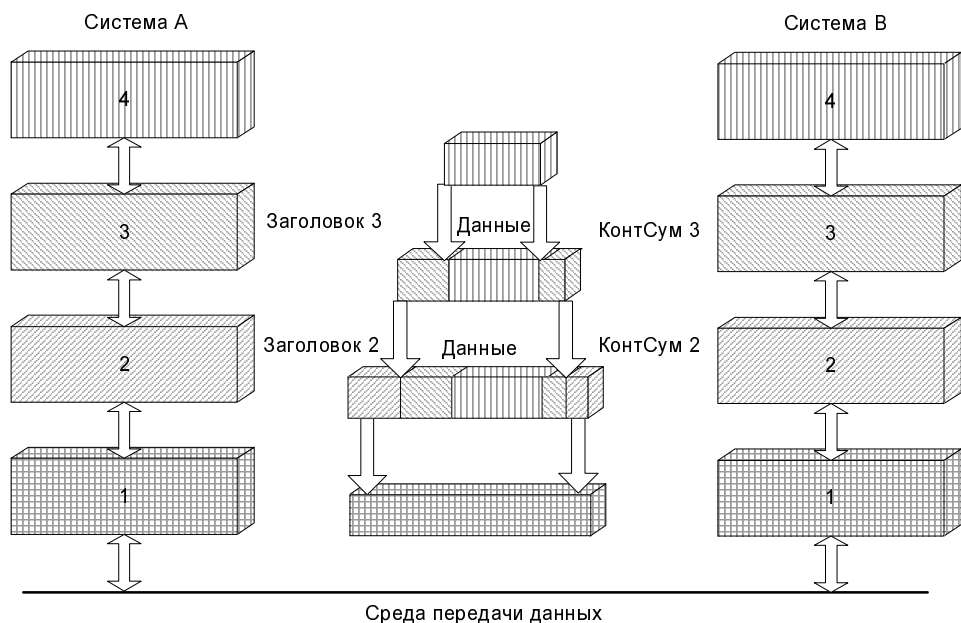


Рис. 1.2. Инкапсуляция блоков данных различных уровней

В соответствии с ISO 7498 выделяются семь уровней (слоев) информационного взаимодействия:

7. Уровень приложения (Application Layer)
6. Уровень представления (Presentation Layer)
5. Уровень сессии (Session Layer)
4. Транспортный уровень (Transport Layer)
3. Сетевой уровень (Network Layer)
2. Канальный уровень (DataLink Layer)
1. Физический уровень (Physical Layer)

Информационное взаимодействие двух или более систем, таким образом, представляет собой совокупность информационных взаимодействий уровне-вых подсистем, причем каждый слой локальной информационной системы взаимодействует только с соответствующим слоем удаленной системы.

Определение

Протоколом мы будем называть набор алгоритмов (правил) взаимодействия объектов одноименных уровней.

Слои (уровни) одной информационной системы также взаимодействуют друг с другом, причем в непосредственном взаимодействии участвуют только соседние уровни. Как правило, средний уровень пользуется услугами, которые ему предоставляет нижний уровень, а сам, в свою очередь, предоставляет услуги для верхнего уровня.

Определение

Интерфейсом мы будем называть совокупность правил, в соответствии с которыми осуществляется взаимодействие с объектом данного уровня.

Иерархическая организация сетевого взаимодействия позволяет обеспечивать преемственность разработанных структур и их быструю адаптацию к изменениям, происходящим в технологиях передачи данных. Например, при переходе на новый способ передачи данных по физическому носителю, изменения коснутся только нижних уровней и совсем не затронут верхние в том случае, если система протоколов организована в соответствии с требованиями ISO 7498. На практике требования данного стандарта реализуются в виде стека протоколов.

Определение

Стеком мы будем называть иерархически организованную группу взаимодействующих протоколов

Протоколы, которые входят в стек, имеют специализированный интерфейс и предназначены для взаимодействия только с протоколами соответствующих уровней данного стека. В качестве примеров таких стеков можно привести стек TCP/IP и протоколы X.25.

Уровни 7—5 считаются верхними и, как правило, не отражают специфики конкретной сети. Блок данных пользователя (сообщение) этими уровнями рассматривается как единое целое. Изменения могут испытывать только сами данные.

Уровни 1—3 и иногда 4 считаются нижними уровнями OSI. На каждом из этих уровней определяется свой формат представления данных. При прохождении по стеку с 4-го уровня до первого сообщение пользователя последовательно фрагментируется и преобразуется в последовательность блоков данных соответствующего уровня.

Определение

Процесс помещения фрагментированных блоков данных одного уровня в блоки данных другого уровня называют *инкапсуляцией*.

Обычно инкапсулируются данные протоколов верхних уровней в блоки данных протоколов нижних уровней (сетевой — канальный), но также может выполняться инкапсуляция для протоколов одноименных уровней (IP-X.25).

Уровень приложения

Протоколы, оперирующие на седьмом уровне OSI, предназначены для обеспечения доступа к ресурсам сети программ-приложений пользователя. На данном уровне определяется интерфейс с коммуникационной частью приложения. В качестве примера протоколов прикладного уровня можно привести протокол TELNET, который обеспечивает доступ пользователя к узлу сети в режиме удаленного терминала.

Уровень представления

На этом уровне обычно выполняется преобразование форматов данных, алгоритмы шифрования и компрессии данных.

Уровень сессии

На данном уровне устанавливаются, обслуживаются и разрываются сессии между представительными объектами приложений. В качестве примера протокола сеансового уровня можно рассмотреть протокол RPC (Remote Procedure Call). Как следует из названия, данный протокол предназначен для отображения результатов выполнения процедуры на удаленном узле. В процессе выполнения этой процедуры между приложениями устанавливается сеансовое соединение. Назначением этого соединения является обслуживание запросов, возникающих при взаимодействии приложения-клиент с приложением-сервер. Протоколы сеансового уровня непосредственно взаимодействуют с протоколами транспортного уровня. Организация сеансового соединения может вызвать установление транспортного соединения. Возможен, однако, вариант, когда несколько сеансовых соединений используют одно транспортное.

Транспортный уровень

Можно выделить два типа протоколов транспортного уровня — сегментирующие протоколы и дейтаграммные протоколы.

Сегментирующие протоколы транспортного уровня разбивают исходное сообщение на блоки данных транспортного уровня — сегменты. Основной функцией таких протоколов является обеспечение гарантированной доставки этих сегментов до объекта назначения и восстановление исходного сообщения. Для выполнения этой задачи протокол транспортного уровня устанавливает и разрывает соединение между узлами, управляет скоростью передачи сегментов и обеспечивает достоверность передачи и восстановления сообщения специальными контрольными процедурами. Функционирование протокола транспортного уровня состоит из трех фаз: фазы установления соединения, фазы передачи сегментов и фазы разрыва соединения.