

Глава 7

Налаживаем взаимодействие между компьютерами: выбор стека протоколов

В этой главе вы найдете ответы на следующие вопросы:

- **Что такое стек протоколов?**
- **Какие существуют стеки протоколов?**
- **Какой стек протоколов наиболее распространен?**
- **Какие протоколы различных уровней используются в TCP/IP?**

В прошлых главах мы узнали, как компьютеры объединяются в сети, выбрали сетевую топологию и архитектуру, соединили компьютеры с помощью коммутаторов (или других устройств связи) и построили драйверы сетевых адаптеров. Однако чтобы компьютеры могли работать в сети, всего этого недостаточно. Теперь нужно научить сетевые приложения «разговаривать» друг с другом — обмениваться данными с помощью протоколов на уровнях, более высоких, чем канальный. Поскольку этих уровней несколько, нам потребуется не один, а несколько протоколов, объединенных в набор, или, как говорят, в *стек*.

В этой главе мы изучим некоторые наиболее часто применяемые в сетях *стеки протоколов*, в том числе самый распространенный на сегодня набор протоколов — *стек TCP/IP*.

Как и в случае с сетевыми архитектурами, начнем изучение с протоколов, которые сейчас применяются достаточно редко.



Аббревиатура NetBEUI расшифровывается как «NetBIOS Extended User Interface» — «улучшенная версия протокола NetBIOS».

NetBEUI

Небольшой по объемам требуемого программного обеспечения протокол, реализующий поддержку *сетевого, транспортного и сеансового уровней* модели OSI. Наиболее прост в настройке (фактически ее не требует), работает эффективно и быстро в небольших и средних по размерам сетях (до 200 компьютеров). Серьезными, по современным меркам, недостатками протокола NetBEUI являются ограничения при работе в сетях с большим количеством компьютеров и, самое главное, отсутствие поддержки маршрутизации — возможности сетевой адресации и функции пересылки пакетов между сетями в нем просто не реализованы. Соответственно, его нельзя использовать в крупных сетях, объединенных маршрутизаторами, и при работе с Интернетом. Протокол NetBEUI поставлялся в составе всех операционных систем Windows вплоть до Windows 2000, однако в последних версиях его поддержка прекращена.

IPX/SPX и NWLink

Стек протоколов IPX/SPX был разработан фирмой Novell в начале 80-х гг. для своей сетевой операционной системы NetWare. Основа стека — это протоколы IPX (Internetwork Packet eXchange) и SPX (Sequenced Packet eXchange), реализующие функции *сетевого и транспортного уровней* модели OSI соответственно. Как и NetBEUI, протокол IPX/SPX является небольшим (его программную поддержку легко уместить на обычной дискете 1,44 Мб вместе с DOS) и быстрым, что было особенно важно в эпоху первого поколения IBM-совместимых компьютеров с малым объемом оперативной памяти (640 Кбайт). Кроме того, в стеке IPX/SPX поддерживается маршрутизация. Оба этих фактора, наряду с надежностью серверов на базе опера-



NWLink — реализация стека IPX/SPX компанией Microsoft, поставляемая во всех версиях Windows.

ционной системы Novell Netware тех лет, способствовали широкому распространению стека IPX/SPX в локальных сетях в 80-е и 90-е гг. К недостаткам этого стека протоколов следует отнести интенсивное использование широковещательных сообщений, серьезно нагружающих сеть, особенно при работе по медленным глобальным каналам. Это обстоятельство, а также то, что стек IPX/SPX принадлежит фирме Novell и для его реализации другим производителям сетевых операционных систем приходилось покупать лицензию, привели в итоге к вытеснению IPX/SPX общедоступным стеком TCP/IP. Важную роль здесь сыграло и то, что все больше организаций в 90-е гг. стало подключаться к Интернету, в котором использовался именно стек TCP/IP, а поддерживать в сети два стека протоколов — лишняя «головная боль» для сетевых администраторов.

TCP/IP

История развития стека TCP/IP (как и история Интернета) началась еще в конце 60-х гг. прошлого, XX века с проекта ARPANet — сети Агентства перспективных исследовательских проектов (Advanced Research Project Agency Network) Министерства обороны США. Поскольку для военных во времена «холодной войны» была особенно важна возможность передачи данных даже в условиях атомных бомбардировок, ARPANet задумывалась как высоконадежная сеть, объединяющая военные, государственные и научные учреждения. Получившаяся в результате сеть и разработанный несколько позже (в 70-х гг.) стек протоколов TCP/IP оказались настолько удачными, что даже после прекращения финансирования проекта ARPANet Министерством обороны продолжали жить и успешно развиваться, создав основы современного Интернета.

Основные преимущества стека TCP/IP перед другими (например, перед стеком IPX/SPX) — более удобная система *сетевой адресации*, возможность *фрагментации пакетов* и очень небольшое количество широковещательных сообщений. Эти преимущества оказались решающими не только при построении глобальных сетей, объединяющих сети с разнородными архитектурами, но и при создании крупных корпоративных сетей. В результате сегодня стек TCP/IP практически вытеснил все остальные — он используется и в небольших домашних сетях, и в глобальной сети Интернет.



Поскольку стек TCP/IP является *общедоступным*, его стандарты (а также просто информационные материалы) публикуются в Интернете в виде специальных документов под названием «RFC» («Request for Comments», «запрос комментариев») с последовательно возрастающим номером. К примеру, спецификация протокола IP опубликована в RFC 791, а протокола HTTP версии 1.1 — в RFC 2616. Первый документ RFC был представлен еще в апреле 1969 г., а сейчас текущие номера RFC перевалили за 4 тысячи.

Стек TCP/IP, в отличие от семиуровневой модели OSI, принято описывать в рамках четырех уровней (рис. 7.1).

- *На физическом уровне* TCP/IP поддерживает работу с основными технологиями локальных сетей — Ethernet, Token Ring, Wi-Fi, Bluetooth и т. д.
- *На сетевом уровне* располагаются несколько протоколов:
 - *протокол ARP (Address Resolution Protocol)* является звеном, связывающим сетевой уровень с физическим. Он отвечает за преобразование сетевых IP-адресов в аппаратные MAC-адреса;

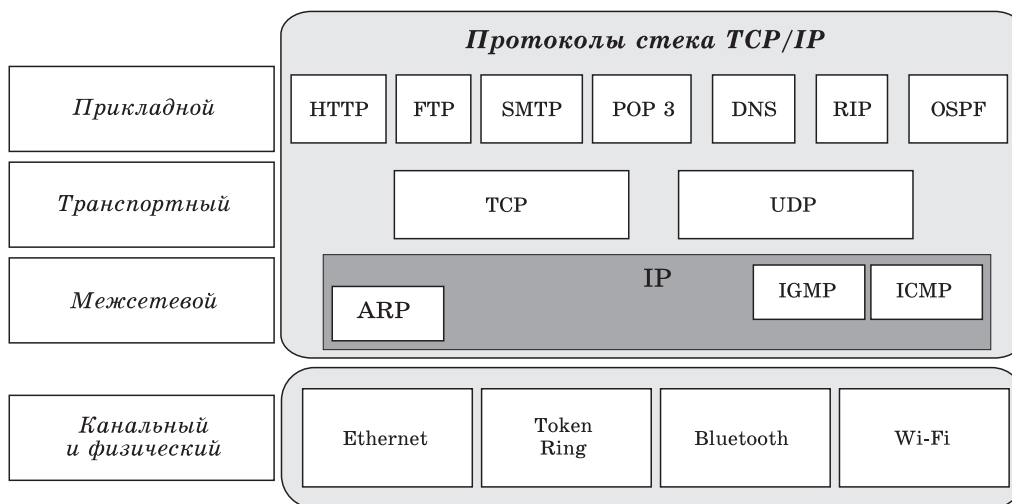


Рис. 7.1. Основные протоколы стека TCP/IP



Проверить, IP-адреса каких компьютеров вашей сети были в последнее время преобразованы в соответствующие им MAC-адреса, можно с помощью команды `ARP -A`.

- *протокол RARP (Reverse Address Resolution Protocol)* — осуществляет обратное преобразование MAC-адресов в IP-адреса (в операционных системах Windows поддержка протокола RARP не предусмотрена);
- *протокол ICMP (Internet Control Message Protocol)* — используется для передачи сообщений об ошибках, диагностики доступности сетевого узла и маршрута доставки пакетов (именно его используют такие популярные утилиты, как PING и TRACERT);
- *протокол IGMP (Internet Group Management Protocol)* — используется для управления группами компьютеров, например, при передаче в сетях потокового видео и звука, когда для снижения нагрузки на сеть пакет посылается по специальному адресу сразу нескольким компьютерам (*многоадресная рассылка*);

- *протокол IP (Internet Protocol)* — один из самых важных в стеке TCP/IP. Как следует из его названия («IP» переводится как «межсетевой протокол»), он отвечает за доставку *IP-дейтаграмм* (так правильно называются пакеты на уровне протокола IP), обеспечивая передачу пакета из одной сети в другую. О том, как это происходит, будет подробно рассказано далее.

➤ *На транспортном уровне работают два протокола:*

- *протокол TCP (Transmission Control Protocol, протокол управления передачей)* — основной протокол транспортного уровня. Обеспечивает *установку соединения* между отправителем и получателем, *разбиение крупного блока информации* (например, файла) на *небольшие TCP-пакеты* и их *гарантированную доставку* получателю (в нужном порядке и без ошибок). Соответственно, протокол TCP используется в тех приложениях, где важно обеспечить целостность при передаче данных;
- *протокол UDP (User Datagram Protocol)*, в отличие от TCP, не устанавливает соединения перед передачей информации и не обеспечивает надежной доставки данных, работая при этом быстрее, чем TCP. Его используют там, где обеспечение доставки информации не особенно важно по сравнению со скоростью передачи (контроль за целостностью данных в этом случае возлагается на использующее протокол UDP приложение).

Чтобы лучше представить себе работу протоколов TCP и UDP, вернемся к нашей аналогии с почтой. Пусть вам надо переслать в издательство целый роман, а в письмо разрешается вкладывать не больше нескольких страниц текста. Чтобы в такой

ситуации ничего не потерять при пересылке и не перепутать при приеме рукописи в печать, вначале хорошо бы договориться с издательством о системах обозначения именно для вашего романа (есть ведь и другие авторы!) и о нумерации сообщений. Для этого нужно послать письмо, извещающее издательство о вашем намерении переслать роман, в котором указать исходящий номер вашего следующего сообщения. Издательство подтвердит получение вашего сообщения и в ответном письме сообщит вам свои исходящие и входящие номера, а вы подтвердите получение этих номеров. Таким образом, обе стороны согласуют номера сообщений, которые они позже будут ожидать друг от друга, что и означает установку связи. Дальше вам остается только разделить роман на небольшие части и послать каждую в отдельном письме, а издательству — подтвердить получение этих частей. Ошибки работы почты (если какое-то сообщение не дойдет до издательства из-за потери или повреждения письма либо придет вне очереди) легко определить по входящим и исходящим номерам, чтобы принять соответствующие меры — заново переслать утерянную часть или собрать страницы романа в нужном порядке.

Примерно так же работает и протокол TCP:

- устанавливает соединение между компьютерами по определенным портам;
- на компьютере-отправителе разбивает информацию на пакеты, нумерует их и с помощью протокола IP передает получателю;
- на компьютере-получателе проверяет, все ли пакеты получены, а если пакет пропущен или поврежден, запрашивает у отправителя повторную пересылку;

- после получения всех пакетов закрывает соединение, собирает пакеты в нужном порядке и передает полученные данные приложению более высокого уровня.

Протокол же UDP в этой аналогии можно сравнить с рассылкой рекламных сообщений. Никакого установления связи и подтверждения получения корреспонденции здесь нет — письма с рекламной информацией просто бросают в ваш почтовый ящик. При этом ни отправителя, ни получателя надежность доставки информации или ее целостность, вообще говоря, не особенно беспокоят.

Очевидно, почтовые отправления в обоих этих примерах являются аналогами IP-пакетов, а почтальоны выполняют функции протокола IP.



Порт в TCP или UDP — это логический канал с определенным номером (от 0 до 65536), обеспечивающий текущее взаимодействие между отправителем и получателем. Порты позволяют компьютеру с одним IP-адресом параллельно обмениваться данными с множеством других компьютеров. Некоторые номера портов (так называемые «хорошо известные», или «well-known», порты с номерами от 0 до 1024) привязаны к определенным службам и приложениям, что позволяет клиентам легко обращаться к нужным им сетевым сервисам.

Наконец, самым богатым по набору протоколов является *прикладной уровень* стека TCP/IP. Ниже в табл. 7.1 приведены самые популярные протоколы, а также зарезервированные для них порты. Заметим, что, хотя для протоколов обычно резервируются одинаковые номера портов и для TCP, и для UDP, в таблице приведены порты для наиболее часто применяемого протокола транспортного уровня (TCP или UDP).

Таблица 7.1

Протоколы прикладного уровня стека TCP/IP

Протокол	Назначение	Номер порта
NTP (Network Time Protocol)	Протокол сетевого времени, используется для синхронизации системных часов компьютеров в сетях	123 (UDP)
DNS (Domain Name System, или Service)	Служба доменных имен, используется для преобразования (разрешения) понятных людям имен компьютеров (например, имен типа www.microsoft.com) в IP-адреса	53 (TCP и UDP)
NetBIOS name service и WINS (Windows Internet Naming Service)	Служба имен NetBIOS и служба межсетевых имен Windows, используются для преобразования NetBIOS-имен компьютеров (например, имен типа SERVER) в IP-адреса	137 и 138 (UDP)
NetBIOS session service	Служба сеансов NetBIOS, используется для установления сеансов между компьютерами	139 (TCP)
LDAP (Lightweight Directory Access Protocol)	Простой протокол доступа к каталогу, используется для работы с различными сетевыми каталогами (например, со службой Active Directory в доменах на основе Windows Server 2003)	389 (TCP)
RPC (Remote Procedure Call)	Вызов удаленной процедуры, используется для работы со многими сетевыми службами в сетях Майкрософт	135 (TCP)
Telnet	Протокол для обеспечения терминального доступа к удаленным компьютерам	23 (TCP)
FTP (File Transfer Protocol)	Протокол передачи файлов, один из «старейших» протоколов Интернета; используется для эффективной и надежной передачи файлов между клиентом и сервером FTP	20 и 21 (TCP)
TFTP (Trivial File Transfer Protocol)	Упрощенный вариант FTP, не имеет таких функций, как проверка пользователя при входе, просмотр каталогов и файлов сервера; используется только для записи и чтения файлов	69 (UDP)

Протокол	Назначение	Номер порта
Gopher	Протокол Gopher («суслик»), используется для доступа к текстовым информационным ресурсам на удаленном сервере	70 (TCP)
HTTP (HyperText Transfer Protocol)	Протокол передачи гипертекста, самый популярный сегодня протокол, используемый во Всемирной паутине (World Wide Web); описывает, каким способом нужно представлять данные (текстовые, аудио-, видео- и т. д.) на веб-серверах, как к ним обращаться с помощью веб-браузера (например, программы Internet Explorer) и как передавать эти данные	80 (TCP)
NNTP (Network News Transfer Protocol)	Протокол передачи сетевых новостей, используется для обмена сообщениями в системах телеконференций	119 (TCP)
SMTP (Simple Mail Transfer Protocol)	Простой протокол передачи почты, используется почтовыми серверами для обмена электронными сообщениями (на этапе отправки почтового сообщения его автором)	25 (TCP)
POP3 (Post Office Protocol)	«Протокол почтового отделения», довольно простой протокол, используемый почтовым клиентом (например, программой Outlook Express) для подключения к своему почтовому ящику на сервере и считывания сообщений (на этапе доставки почтового сообщения адресату)	110 (TCP)
IMAP4 (Internet Message Access Protocol)	Протокол доступа к электронным сообщениям — более функциональный, чем POP3, клиентский протокол для доступа к почтовому серверу	143 (TCP)
SSL (Secure Sockets Layer)	Протокол, обеспечивающий согласование алгоритмов и обмен ключами шифрования. Используется для защиты данных при их пересылке по сетям	25 (SMTP) 995 (POP3S) 993 (IMAPS) 443 (HTTPS) (TCP)



Несмотря на существование большого количества наборов протоколов, основным сегодня является общедоступный стек TCP/IP. Он используется практически повсеместно, начиная с небольших домашних сетей и заканчивая крупнейшей сетью — Интернетом.



Чтобы посмотреть, какие порты на вашем компьютере используются или ожидают подключения, достаточно выполнить команду `NETSTAT -AN`.

На физическом уровне стек TCP/IP поддерживает работу со всеми основными сетевыми технологиями локальных и глобальных сетей, на сетевом — обеспечивает логичную систему адресации и эффективной межсетевой маршрутизации, на транспортном уровне — протоколы как гарантированной, так и быстрой доставки данных, а на уровне приложений — целую гамму разнообразных протоколов.

Поэтому мы рекомендуем использовать в сети именно стек TCP/IP.



Вопросы для повторения

1. Что такое набор (стек) протоколов? В чем смысл термина «стек»?
2. Какие наборы протоколов вы знаете? Чем они различаются?
3. Какой стек протоколов сегодня наиболее популярен? Почему?
4. Какие уровни модели OSI поддерживаются в стеке протоколов TCP/IP?
5. В чем сходство и различие между протоколами TCP и UDP? Когда какой из этих протоколов рекомендуется использовать?
6. Перечислите известные вам протоколы прикладного уровня в стеке TCP/IP. Для чего предназначен каждый из них?
7. Что такое «порт» в TCP/IP? Для чего нужны порты?
8. Какой из транспортных протоколов стека TCP/IP вы бы использовали:
 - для пересылки по сети Интернет архивных файлов?
 - для реализации IP-телефонии (передачи голосовых сообщений в реальном времени) между пользователями двух мобильных компьютеров (ПК), соединенных по беспроводному каналу Wi-Fi?