**Протокол управляющих сообщений Интернета**

Протокол ICMP, спецификация которого изложена в стандарте RFC 792, используется хостами и маршрутизаторами для обмена информа­цией сетевого уровня друг с другом. Чаще всего протокол ICMP приме­няется для передачи сообщений об ошибках. Например, если у нас рабо­тает сеанс Telnet, FTP или HTTP, то мы можем получить сообщение об ошибке «Destination network unreachable» («Сеть назначения недости­жима»). Это сообщение относится именно к протоколу ICMP. В какой-то момент IP-маршрутизатор не смог найти путь к хосту, указанному в вашем приложении Telnet, FTP или HTTP. Тогда маршрутизатор соз­дал и отослал вашему хосту сообщение типа 3 протокола ICMP, указав в сообщении эту ошибку.

ICMP зачастую считается частью протокола IP, однако с архитек­турной точки зрения он располагается прямо над IP, поскольку сообще­ния ICMP передаются внутри IP-дейтаграмм. Таким образом, IP пере­носит сообщения ICMP в качестве своей полезной нагрузки так же, как он переносит сегменты TCP или UDP. Аналогично, если хост получает IP-дейтаграмму, для которой ICMP указан в качестве протокола верх­него уровня, IP демультиплексирует содержимое дейтаграммы в ICMP, точно так же, как он мог бы демультиплексировать эту информацию в TCP или UDP

Сообщения ICMP имеют тип и поле с кодом, а также содержат за­головок и первые 8 байт той IP-дейтаграммы, из-за которой и было сгенерировано ICMP-сообщение (таким образом, отправитель сможет определить, какая дейтаграмма вызвала ошибку). Некоторые типы ICMP-сообщений показаны на рис. 4.23. Обратите внимание: ICMP-сообщения используются не только для сигнализации о возникновении ошибок.

|  |  |  |
| --- | --- | --- |
| **Тип ICMP** | **Код** | **Описание** |
| **0** | **0** | Эхо-отклик (на команду ping) |
| **3** | **0** | Сеть назначения недостижима |
| **3** | **1** | Хост назначения недостижим |
| **3** | **2** | Протокол назначения недостижим |
| **3** | **3** | Порт назначения недостижим |
| **3** | **6** | Сеть назначения неизвестна |
| **3** | **7** | Хост назначения неизвестен |
| **4** | **0** | Подавление источника (борьба с перегрузками) |
| **8** | **0** | Эхо-запрос |
| **9** | **0** | Объявление маршрутизатора |
| **10** | **0** | Обнаружение маршрутизатора |
| **11** | **0** | Предписанное время жизни истекло |
| **12** | **0** | Недопустимый IP-заголовок |

**Рис. 4.23. Типы сообщений протокола ICMP**

Хорошо известная программа ping посылает ICMP-сообщение типа 8 с кодом 0 на указанный хост. Хост назначения, получив этот эхо-запрос, посылает в ответ сообщение ICMP типа 0 с кодом 0. Большинство реали­заций протокола TCP/IP поддерживают сервер ping непосредственно в операционной системе, то есть сервер не является процессом. Обратите внимание: клиентская программа должна иметь возмож­ность проинструктировать операционную систему, что той следует сге­нерировать сообщение ICMP типа 8 с кодом 0.

Еще одно интересное сообщение ICMP — это «подавление источ­ника». Оно редко применяется на практике. Изначально это сообщение предназначалось для контроля над перегрузками — если маршрутизатор начинает пробуксовывать, то он может послать на хост — источник тра­фика — по протоколу ICMP такое сообщение и тем самым принудитель­но снизить скорость передачи данных с хоста. Ранее мы узнали, что протокол TCP обладает собственным механизмом борьбы с перегруз­ками, который работает на транспортном уровне. Таким образом, при борьбе с перегрузками обратной связи на сетевом уровне, в частности, отпадает необходимость применять сообщения о подавлении источника по протоколу ICMP.

Так же мы познакомились с программой Traceroute, которая позво­ляет отслеживать маршрут с хоста к любому другому хосту в мире. Ин­тересно, что программа реализуется с применением сообщений ICMP. Для определения имен и адресов маршрутизаторов между исходным и конечным хостами программа Traceroute на исходном хосте посылает на хост назначения серию обычных IP-дейтаграмм. Каждая из этих дей­таграмм содержит UDP-сегмент с маловероятным номером UDP-порта. Первая имеет предписанное время жизни (TTL) равное 1 «переходу», вторая — 2 «переходам», третья — 3 «переходам» и т. д.

Кроме того, исходный хост запускает таймеры для каждой из дей­таграмм. Когда n-ная дейтаграмма прибывает на n-ный маршрутизатор, он наблюдает, что предписанное время жизни этой дейтаграммы толь­ко что истекло. По правилам протокола IP маршрутизатор избавля­ется от дейтаграммы и посылает исходному хосту предупредительное сообщение ICMP (тип 11, код 0). В этом сообщении содержится имя маршрутизатора и его адрес. Когда оно прибывает на исходный хост, тот определяет по таймеру время, затраченное на путь в оба конца, а также имя и IP-адрес n-ного маршрутизатора (эту информацию он получает из ICMP-сообщения).

Как программа Traceroute с исходного хоста узнает, когда следу­ет прекратить отсылать UDP-сегменты? Вспомните о том, что хост-отправитель постепенно увеличивает значение в поле TTL (предписан­ное время жизни) для каждой последующей отсылаемой дейтаграммы. Соответственно, рано или поздно одна из дейтаграмм попадет на хост-получатель. Поскольку эта дейтаграмма содержит UDP-сегмент с маловероятным номером порта, хост-получатель посылает в ответ источнику ICMP-сообщение «порт недостижим» (тип 3 код 3). Ког­да исходный хост получает именно это ICMP-сообщение, он «делает вывод», что больше не требуется отсылать дополнительные зонди­рующие пакеты. (Кстати, стандартная программа Traceroute отсылает наборы из трех пакетов, имеющих одинаковое значение TTL; соответ­ственно, вывод Traceroute содержит по три результата для каждого из значений TTL.)

**О БЕЗОПАСНОСТИ**

**Инспектирование дейтаграмм: брандмауэры и системы обнаружения вторжений**

Допустим, вам поручено администрировать сеть — домашнюю, ве­домственную, университетскую или корпоративную. Злоумышлен­ники, зная диапазон IP-адресов вашей сети, вполне могут отсылать на них дейтаграммы. Эти дейтаграммы могут совершать всевоз­можные вредные операции, в частности выявлять топологию вашей сети при помощи эхо-тестирования адресов и сканирования пор­тов, атаковать уязвимые хосты искаженными пакетами, наводнять серверы потоками ICMP-пакетов, инфицировать хосты, включая в пакеты вредоносное ПО. Что вы, администратор вычислительной сети, можете противопоставить всем этим злоумышленникам, каж­дый из которых может посылать в вашу сеть вредоносные пакеты? Два популярных механизма защиты, позволяющих предохранить сеть от атак вредоносными пакетами — это брандмауэры и системы обнаружения вторжения (IDS).

Вы как администратор вычислительной сети, вероятно, первым делом попробуете установить брандмауэр (сетевой экран) между вашей сетью и Интернетом. Большинство современных маршру­тизаторов доступа оснащены функцией брандмауэра. Он анализи­рует дейтаграммы и сегментирует поля заголовков, предотвращая проникновение подозрительных дейтаграмм во внутреннюю сеть. Например, он может быть сконфигурирован так, что будет блокиро­вать все ICMP-пакеты, содержащие эхо-запросы. Это лишит злоу­мышленника возможности выполнить в вашем диапазоне IP тра­диционное эхо-тестирование адресов. Брандмауэры также могут блокировать пакеты в зависимости от их исходного и конечного IP-адресов и номеров портов. Кроме того, они могут иметь специаль­ную конфигурацию для отслеживания TCP-соединений и допускать в сеть только те дейтаграммы, которые получены через доверенные соединения.

Дополнительная защита обеспечивается при помощи систем обна­ружения вторжений (IDS). Система IDS, которая обычно располага­ется на границе сети, выполняет «глубокую проверку пакетов», при которой учитываются не только поля заголовков, но и поля данных дейтаграмм (включая данные прикладного уровня). В системе IDS есть база данных сигнатур тех пакетов, при помощи которых совер­шались известные ей атаки. База данных автоматически обновляет­ся по мере обнаружения новых атак. Когда пакеты проходят через систему IDS, система пытается сопоставить их поля заголовков и данных с теми сигнатурами, которые перечислены в ее базе дан­ных. Как только фиксируется такое совпадение, система генерирует предупредительное сообщение. Существуют также системы пре­дотвращения вторжений (IPS), подобные IDS, с той оговоркой, что система IPS не только генерирует предупреждения, но и блокирует подозрительные пакеты.

Могут ли брандмауэры и системы обнаружения вторжений полно­стью защитить вашу систему от всех возможных атак? Разумеется, нет, поскольку злоумышленники постоянно изобретают новые атаки. сигнатуры которых еще не зафиксированы. Но брандмауэры и тра­диционные системы IDS, работающие на основе сравнения сигна­тур, хорошо защищают системы от известных атак.

Таким образом, исходный хост узнает, сколько маршрутизаторов находится между ним и конечным хостом, а также уникальные иден­тификаторы этих маршрутизаторов и время, затрачиваемое на путь туда и обратно между двумя хостами. Обратите внимание: клиентская программа Traceroute должна иметь возможность потребовать от опе­рационной системы генерировать UDP-дейтаграммы с конкретными значениями TTL (предписанного времени жизни), а также получать от своей операционной системы уведомления о поступлении сообщений протокола ICMP. Теперь, разобравшись в принципах работы програм­мы Traceroute, вам, возможно, захочется вернуться назад и еще немного поэкспериментировать с ней.

**IPv6**

В начале 1990-х организация IETF (Инженерный совет Интернета) приступила к разработке протокола, призванного заменить IPv4. Основ­ным мотивом для этой работы стало растущее понимание того, что 32-битное пространство IP-адресов достаточно скоро будет израсходова­но в силу распространения новых подсетей и IP-узлов, подключаемых к Интернету. Присвоение новых уникальных IP-адресов становилось невероятно стремительным. Чтобы удовлетворить острую потребность в них, был разработан новый протокол — IPv6. Создатели IPv6 также не преминули усовершенствовать и дополнить другие аспекты протокола IPv4, опираясь на богатый накопленный опыт его эксплуатации.

Ведутся активные споры относительно того, когда все адреса IPv4 будут израсходованы (и, соответственно, исчезнет возможность под­ключения новых сетей к Интернету). Выводы двоих ведущих специалистов рабочей группы IETF по оценке времени, оставшегося до оконча­тельного истощения адресного пространства, указывали на 2008 либо на 2018 год соответственно. В феврале 2011 года организация IANA (Ад­министрация адресного пространства Интернета) выделила последний пул не присвоенных адресов IPv4 региональному регистратору. В рас­поряжении региональных Интернет-регистраторов по-прежнему есть свободные адреса IPv4, но когда все они будут израсходованы, больше не останется ни одного блока адресов, который можно было бы допол­нительно выделить из центрального пула. Хотя в середине 1990-х счи­талось, что полное истощение адресного пространства IPv4 произойдет еще достаточно нескоро, разработчики в то же время, понимали, что на разработку новой технологии такого масштаба потребуется очень зна­чительное время. Поэтому был запущен проект «Новое поколение IP» (IPng). Результатом этих разработок стало создание специфика­ции протокола IP версии б (IPv6), о которой мы подробно поговорим ниже. Здесь часто задают вопрос: а почему же так и не появился прото­кол IPv6? Первоначально предполагалось, что роль IPv6 уготована про­токолу ST-2, но позже от ST-2 было решено отказаться.

**Формат дейтаграмм IPv6**

Формат дейтаграмм IPv6 проиллюстрирован на рис. 4.24. Самые важные изменения, отличающие IPv6, очевидны именно в формате дей­таграмм.

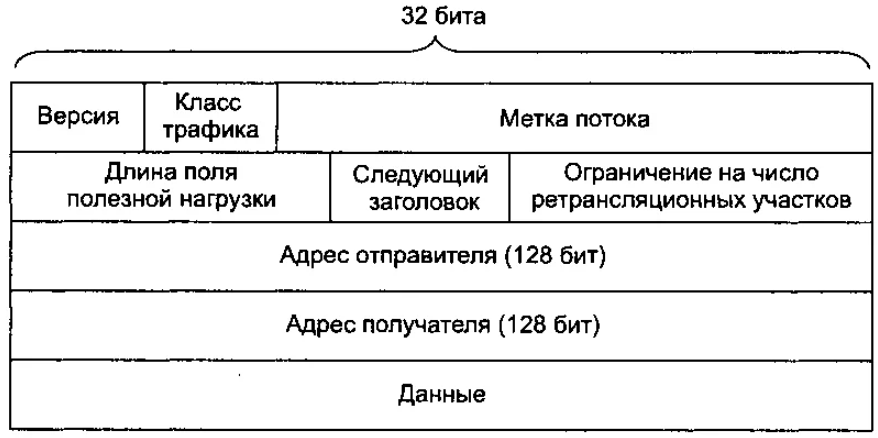
* ***Расширенные возможности адресации.* В протоколе IPv6 размер IP-**адреса увеличивается с 32 до 128 бит. Таким образом гарантируется, что IP-адреса в мире не закончатся никогда. Теперь можно присво­ить IP-адрес каждой песчинке на нашей планете. В IPv6 появился новый тип адреса, именуемый **адресом свободной рассылки,** кото­рый позволяет доставить дейтаграмму любому хосту из указанной группы. Например, эту возможность удобно применять для отправ­ки HTTP-запроса GET ближайшему сайту-зеркалу из нескольких имеющихся, на котором содержится искомый документ.
* ***Оптимизированный 40-байтный заголовок.* Как будет указано ниже,** ряд полей IPv4 были упразднены или сделаны необязательными. В результате получились заголовки, имеющие фиксированную длину в 40 байт и обеспечивающие более быструю обработку IP-дейтаграмм. Новая кодировка возможностей обеспечивает их уско­ренную обработку.

Рис. 4.24. Формат дейтаграммы IPv6

• *Метка потока и приоритет.* В протоколе IPv6 существует доволь­но туманное определение потока. В стандартах RFC 1752 и RFC 2460 записано, что данная сущность обеспечивает «пометку паке­тов, относящихся к конкретным потокам, для которых отправи­тель затребует специальной обработки — например, обслуживания в локальном времени или качества обслуживания, отличающегося от заданного по умолчанию». Например, передача аудио или видео может интерпретироваться как поток. С другой стороны, при реше­нии более традиционных задач — например, при передаче файлов и электронной почты — сообщаемая информация может и не об­рабатываться как потоки. Возможна ситуация, в которой пользова­тельский трафик с высоким приоритетом (например, если пользо­ватель доплатил за более качественное обслуживание) также будет обрабатываться как поток. Так или иначе, совершенно очевидно, что создатели IPv6 предвидели: рано или поздно потребуется механизм различения потоков, пусть даже точное определение самого тер­мина пока отсутствует. Кроме того, в заголовке IPv6 есть 8-битное поле класса трафика. Это поле, как и поле TOS (тип сервиса обслу­живания) в IPv4, может применяться для присвоения приоритета определенным дейтаграммам в потоке либо для предпочтения дей­таграмм, исходящих от одних приложений (допустим, от протокола ICMP) дейтаграммам от других приложений (таких, как сетевые новости).

Как было указано выше, при сравнении рис. 4.24 и рис. 4.13 легко заметить, что дейтаграмма IPv6 обладает более простой и обтекаемой структурой. В дейтаграммах IPv6 определяются следующие поля:

* *Версия.* Это 4-битное поле указывает номер версии протокола IP. Неудивительно, что в протоколе IPv6 здесь записано значение 6. Правда, следует отметить, что, заменив в этом поле 6 на 4, мы не по­лучим валидную дейтаграмму IPv4. (Если бы такой прием действо­вал, жизнь была бы просто сказкой — см. ниже раздел о переходе с IPv4 на IPv6.)
* *Класс трафика.* Это 8-битное поле функционально напоминает поле TOS (тип обслуживания), знакомое нам по протоколу IPv4.
* *Метка потока.* Как было указано выше, это 20-битное поле приме­няется для идентификации потока дейтаграмм.
* *Размер полезных данных.* Это 16-разрядное значение трактуется как беззнаковое целое число и указывает количество байт в дейтаграмме IPv6, следующих за заголовком; как вы уже знаете, длина заголовка фиксированная и составляет 40 байт.
* *Следующий заголовок.* В этом поле указывается протокол, на кото­рый будет доставлено содержимое (поле с данными) этой дейта­граммы — например, TCP или UDP. В этом поле используются те же значения, что и в поле протокола в заголовке IPv4.
* *Лимит переходов.* Значение, содержащееся в этом поле, уменьшает­ся на единицу каждым из маршрутизаторов, которые пересылают дейтаграмму. Если значение достигает нуля, то дейтаграмма утили­зируется.
* ***Адреса отправителя и получателя.* Различные форматы 128-**разрядного адреса протокола IPv6 описаны в стандарте RFC 4291.
* *Данные.* Это полезное содержимое дейтаграммы IPv6. Когда дейта­грамма достигает места назначения, данные изымаются из нее и пе­редаются протоколу, указанному в поле следующего заголовка.

Выше мы рассмотрели назначение полей, входящих в состав дейта­граммы IPv6. Сравнив формат дейтаграммы IPv6 с рис. 4.24 и формат дейтаграммы IPv4 с рис. 4.13, легко заметить, что некоторые поля дей­таграмм IPv4 в IPv6 отсутствуют:

• *Фрагментация/пересборка:* протокол IPv6 не допускает фрагмента­  
цию и пересборку дейтаграмм на промежуточных маршрутизаторах;  
эти операции могут выполняться лишь на хостах — отправителе и по­  
лучателе. Если дейтаграмма IPv6, полученная маршрутизатором,  
слишком велика, и ее не удается передать по исходящему соединению, то маршрутизатор просто отбрасывает эту дейтаграмму и отсы­лает отправителю по протоколу ICMP сообщение «Packet Too Big» («Пакет слишком велик») (см. ниже). После этого отправитель мо­жет переслать данные, составив более компактную 1Р-дейтаграмму. На фрагментацию и пересборку дейтаграмм тратится немало време­ни; при удалении этой функции с промежуточных маршрутизаторов и локализации только в начальной и конечной системе удается зна­чительно ускорить передачу информации в сети по протоколу IP.

* *Контрольная сумма заголовка.* Поскольку протоколы транспортно­го уровня (TCP и UDP) и канального уровня (например, стандарт Ethernet) в Интернете выполняют проверку контрольных сумм, раз­работчики IP, вероятно, сочли, что на сетевом уровне эта функцио­нальность является избыточной, и ее можно оттуда удалить. Опять же, основное внимание уделялось ускорению обработки IP-пакетов. Как вы помните из обсуждения протокола IPv4, по­скольку в заголовке IPv4 есть поле TTL (Предписанное время жиз­ни), подобное полю лимита переходов в IPv6, контрольная сумма за­головка IPv4 должна пересчитываться на каждом маршрутизаторе. Как и фрагментация/пересборка, такой пересчет был признан слиш­ком затратной операцией.
* *Опции.* Поле опций больше не входит в состав стандартного IP-за­головка. Однако оно не исчезло. Теперь поле опций — это один из ва­риантов поля следующего заголовка, на который содержится указа­ние в IPv6. Таким образом, в качестве следующего заголовка можно указывать как протокол TCP или UDP, так и поле опций. Поскольку поле опций удалено из стандартного заголовка, длина такого IP-за­головка стала фиксированной и составляет 40 байт.

Как вы помните, протокол ICMP используется IP-узлами, чтобы сообщать о состояниях ошибок и предоставлять краткую информацию (например, эхо-отклика на сообщение ping) конечной си­стеме. Для работы с протоколом IPv6 в стандарте RFC 4443 была опре­делена новая версия ICMP. В ICMPv6 были не только реорганизованы имеющиеся определения типов и кодов, но и добавлены новые типы и коды, необходимые для работы с новым функционалом протокола IPv6. Один из таких типов — «Packet Too Big» (Пакет слишком велик), один из новых кодов ошибки — «unrecognized IPv6 options» («Неопо­знанные опции IPv6»). Кроме того, протокол ICMPv6 включает в себя функционал протокола IGMP (протокол управления группами Интер­нета), который мы изучим позднее. Протокол IGMP, управляющий подключением хоста к многоадресным группам и выходом из таких групп, в версии IPv4 был самостоятельным протоколом, не связанным с ICMP.

**Переход с IPv4 на IPv6**

Итак, рассмотрев технические детали протокола IPv6, давайте обсу­дим животрепещущий практический вопрос: как осуществить переход всего общедоступного Интернета с IPv4 на IPv6? Проблема заключает­ся в том, что можно обеспечить лишь обратную совместимость систем, работающих по протоколу IPv6, чтобы они могли посылать, переадресо­вывать и получать дейтаграммы IPv4. Однако уже развернутые систе­мы для работы с IPv4 не смогут обрабатывать дейтаграммы IPv6. Суще­ствует несколько вариантов решения этой проблемы.

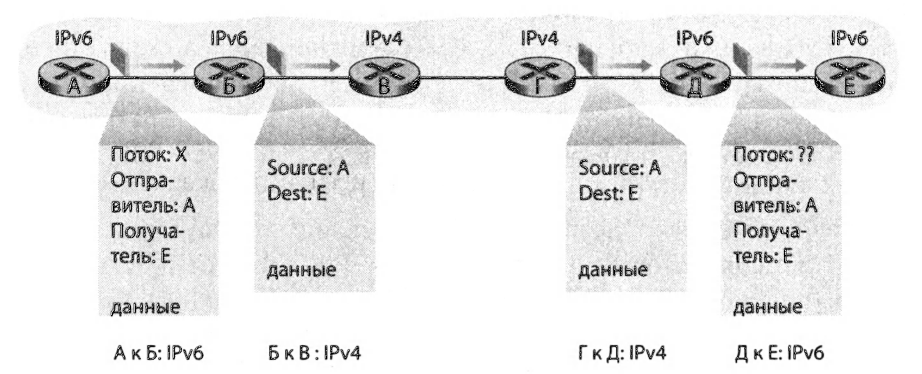
Один из способов — объявить конкретный день (дату и время), в ко­торый все машины Интернета будут отключены и модернизированы с IPv4 до IPv6. Последний технологический переход такого масштаба (переход при передаче данных с протокола NCP на TCP) имел место почти 25 лет назад. Даже в те времена, когда Интернет еще был миниа­тюрным и его администрировала горстка «мастеров», уже стало понятно, что назначить подобное «время Ч» невозможно. Если же экстраполиро­вать такой вариант на наши дни, когда сотни миллионов машин обслу­живает армия администраторов вычислительной сети и эксплуатируют миллионы пользователей, подобное мероприятие кажется тем более не­мыслимым. В стандарте RFC 4213 описаны два способа (которые могут использоваться совместно или по отдельности) для постепенной инте­грации хостов и маршрутизаторов IPv6 в мир IPv4. Долгосрочная цель такой операции — полный отказ от всех узлов IPv4 и окончательный переход на IPv6.

Вероятно, наиболее прямолинейным способом вести узлы с под­держкой IPv6 является так называемый подход **двойного стека,** где узлы IPv6 также оснащаются полноценной реализацией поддержки IPv4. Такой узел, именуемый IPv6/IPv4 в стандарте RFC 4213, может отсылать и принимать дейтаграммы сразу в двух форматах: IPv6 и IPv4. При взаимодействии с узлом IPv4 узел IPv6/IPv4 может использовать дейтаграммы IPv4, при работе с IPv6 — «говорить на языке» IPv6. Узлы IPv6/IPv4 должны обладать адресами как IPv6, так и IPv4. Кроме того, они должны быть способны определять, для работы с какой версией про­токола предназначен узел-собеседник — IPv4 или IPv6. Эта проблема решаема при помощи системы DNS, которая сможет воз­вращать адрес IPv6, если разрешаемое имя узла оказывается пригодным к работе с IPv6, а в противном случае — возвращать именно адрес IPv4.

В случае двойного стека дейтаграммы IPv4 используются, если от­правитель или получатель пакетов поддерживает только IPv4. В резуль­тате может сложиться ситуация, в которой, в сущности, дейтаграммами IPv4 будут обмениваться два узла, поддерживающие IPv6. Такая про­блема проиллюстрирована на рис. 4.25. Предположим, узел А поддержи­вает IPv6, и ему нужно отослать дейтаграмму на узел Е, который также поддерживает IPv6. Узлы А и Б могут обменяться дейтаграммой IPv6. Однако узел Б должен создать дейтаграмму IPv4, чтобы отправить ее на узел В. Конечно же, поле данных дейтаграммы IPv6 можно скопировать в поле данных дейтаграммы IPv4 и выполнить соответствующее со­вмещение по адресу. Однако при преобразовании дейтаграммы из IPv6 в IPv4 те поля, которые специфичны для IPv6 (например, поле иден­тификатора потока), не будут иметь аналогов в IPv4. Информация из этих полей окажется потеряна. Соответственно, даже при том, что узлы Д и Е могут обмениваться дейтаграммами IPv6, дейтаграмма IPv4, ко­торая придет на узел Д с узла Г, не будет содержать все те поля, которые были в исходной дейтаграмме IPv6, посланной с узла А.

Альтернатива применению двойного стека, также рассмотренная в RFC 4213 — это так называемое **туннелирование.** Оно позволяет решить вышеописанную проблему, обеспечивая, допустим, получение узлом Д тех дейтаграмм IPv6, которые были отосланы с узла А. Базовая идея, на которой построен механизм туннелирования, такова. Предположим, два узла поддерживают работу по протоколу IPv6 (на рис. 4.25 это, например, узлы Б и Д). Им требуется взаимодействовать, обмениваясь дейтаграмма­ми IPv6, однако между ними находятся маршрутизаторы, поддерживаю­щие только IPv4. Этот ряд промежуточных IPv4-Mаршрутизаторов между IPv6-хостами называется **туннель,** см. рис. 4.26. При использовании тун­нелирования узел IPv6, находящийся на стороне отправителя (например, узел Б), принимает *всю* дейтаграмму IPv6 и записывает ее в поле данных (полезной нагрузки) дейтаграммы IPv4.

Затем эта дейтаграмма IPv4 пересылается на узел IPv6 на той сторо­не туннеля, где находится получатель (например, на узел Д) и отправ­ляется на первый узел в туннеле (например, В). Промежуточные марш­рутизаторы IPv4, расположенные в туннеле, пересылают дейтаграмму IPv4 лишь между собой, как и любую другую, совершенно «не подозревая», что полезными данными такой IPv4-дейтаграммы является целая дейтаграмма IPv6. Узел IPv6 на той стороне туннеля, где находится по­лучатель, наконец получает дейтаграмму IPv4 (действительно, ведь это ее место назначения!), определяет, что в качестве данных она содержит дейтаграмму IPv6, извлекает дейтаграмму ее, а затем пересылает точно так же, как если бы получил напрямую с одного из узлов, расположен­ных на стороне отправителя.

■

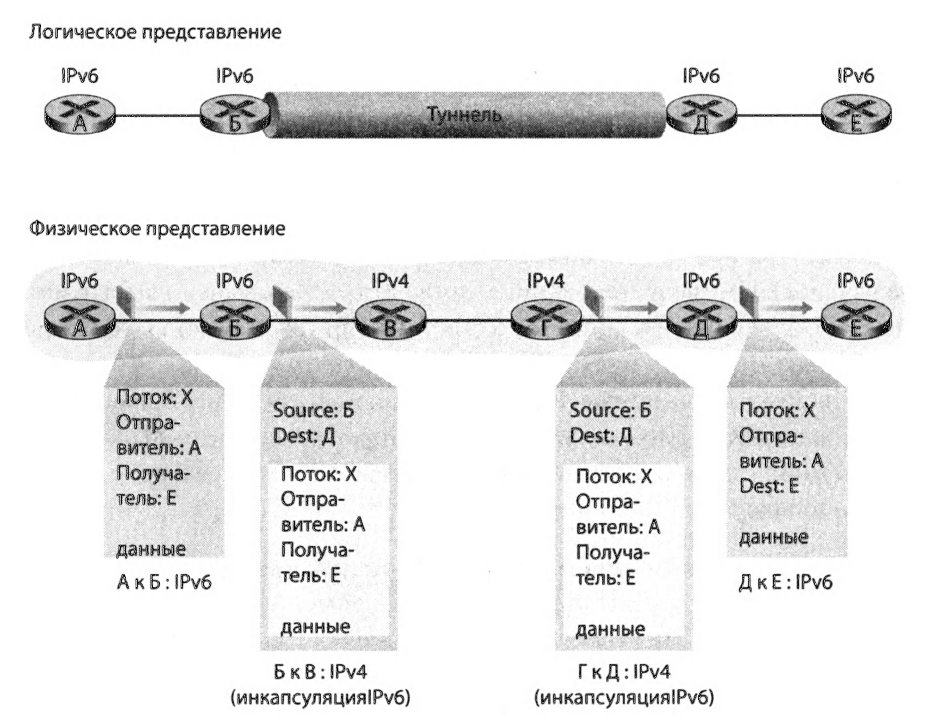
Рис. 4.25. Подход с применением двойного стека

Рис. 4.26. Туннелирование

Отметим, что, хотя переход на IPv6 поначалу протекал медленно, недавно этот процесс стал ускоряться. Распространение новых устройств — например, смартфонов с выходом в Интернет и другой мобильной техники — создает дополнительный импульс для все более широкого распространения IPv6. Европейская «Программа партнерства в области технологий третьего поколения»указывает IPv6 как стандартную схему адресации для мобильных муль­тимедиа.

Важный вывод, который мы можем сделать из опыта работы с IPv6, заключается в том, что на практике исключительно сложно менять про­токолы сетевого уровня. С самого начала 1990-х не раз провозглаша­лось, что очередной новый протокол совершит революцию в Интерне­те, но до сих пор большинство из них получили весьма ограниченное распространение. В частности, к таким протоколам относятся IPv6, протоколы групповой адресации и протоколы резервирования ресурсов. Действительно, ввод новых протоколов на сетевом уровне можно сравнить с заменой фундамента в многоквар­тирном доме. Решить эту задачу очень сложно, если не сносить сам дом и не выселять из него всех жильцов — как минимум, временно. С другой стороны, в истории Интернета известны случаи стремительного раз­вертывания новых протоколов на прикладном уровне. Классические примеры — Всемирная паутина, протокол обмена мгновенными сооб­щениями, одноранговый обмен файлами. Также можно упомянуть по­токовую передачу аудио и видео и распределенные игры. Добавление новых протоколов прикладного уровня можно сравнить с очередной покраской дома. Сделать это относительно просто, а если вы подбере­те красивый оттенок, то вашему примеру последуют соседи по району. Итак, в будущем вполне могут произойти изменения на сетевом уровне Интернета, но они определенно будут протекать гораздо медленнее, чем сопоставимые изменения на прикладном уровне.

**Краткое знакомство с IP-безопасностью**

Ранее мы довольно подробно рассмотрели протокол IPv4 — в частности, обсудили, какие службы он предоставляет, и как реали­зуются эти службы. Протокол IPv4 разрабатывался в эпоху (1970-е), когда Интернет ис­пользовался преимущественно в узком кругу ученых, исследователей сетей, где все друг друга знали и пользовались взаимным доверием. В те годы само создание компьютерной сети, объединяющей в себе множе­ство технологий канального уровня, было задачей не из легких, что уж говорить об обеспечении безопасности.

Но сегодня проблемы безопасности стали исключительно актуаль­ны, и исследователи Интернета приступили к разработке новых прото­колов сетевого уровня, предусматривающих целый комплекс служб по обеспечению безопасности. Один из наиболее популярных протоколов из этой категории называется IPsec, и, кстати, очень активно внедряется в виртуальных частных сетях (VPN). Хотя сам IPsec и его криптографи­ческие основы довольно подробно рассмотрены позднее, сейчас мы предлагаем краткое общее введение, в котором расскажем о службах IPsec.

Протокол IPsec проектировался так, чтобы в нем обеспечивалась об­ратная совместимость с протоколами IPv4 и IPv6. В частности, чтобы полностью пользоваться преимуществами IPsec, нам не требуется заме­нять стеки протоколов во *всех* маршрутизаторах и хостах в Интернете. Например, при работе в транспортном режиме IPsec (это один из двух его «режимов»), если двум хостам требуется безопасно обмениваться информацией по этому протоколу, то он должен действовать лишь на этих двух хостах. Все остальные маршрутизаторы и хосты, расположен­ные между ними, могут использовать тривиальный IPv4.

Ради конкретизации изложения мы поговорим здесь только о транс­портном режиме IPsec. В таком режиме два хоста сначала устанавливают друг с другом сеанс IPsec. (Таким образом, протокол IPsec ориентиро­ван на соединения!) Когда сеанс установлен, все сегменты TCP и UDP, пересылаемые между этими хостами, в полной мере могут использовать службы IPsec. Co стороны отправителя транспортный уровень пере­дает сегмент по протоколу IPsec. Затем IPsec шифрует сегмент, при­крепляет к нему дополнительные поля, необходимые для обеспечения безопасности, после чего инкапсулирует эти данные в самую обычную IP-дейтаграмму. (На самом деле весь этот процесс немного сложнее.) Затем хост-отправитель отсылает дейтаграмму в Интернет, который уже обеспечивает ее доставку хосту-получателю. Там IPsec расшифровывает сегмент и незашифрованным передает его на транспортный уровень.

В ходе сеанса с применением IPsec предоставляются следующие службы.

* *Криптографическое соглашение.* Это механизм, позволяющий двум хостам согласовать криптографические ключи и алгоритмы, кото­рые будут применяться при обмене информацией.
* *Шифрование* полезного содержимого *IP-дейтаграмм.* Когда хост-отправитель получает сегмент через транспортный уровень, прото­кол IPsec шифрует данные. Дешифровать их может лишь протокол IPsec на хосте-получателе.
* *Целостность данных.* Протокол IPsec позволяет хосту-получателю проверить поля заголовка дейтаграммы и узнать, не было ли по­лезное содержимое изменено, пока дейтаграмма находилась в пути.

*Аутентификация источника.* Когда хост получает дейтаграмму по протоколу IPsec из доверенного источника (с доверенным ключом), он может быть уверен, что дейтаграмма пришла именно с того IP-адреса, который указан в качестве ее источника.

Когда между двумя хостами установлено соединение по протоколу IPsec, все пересылаемые между ними фрагменты TCP и UDP шифруют­ся и аутентифицируются. Соответственно, протокол IPsec обеспечивает сплошной охват, гарантируя безопасность любого соединения между двумя хостами, какие бы сетевые приложения при этом ни применя­лись.

Компания может использовать протокол IPsec, чтобы безопасно обмениваться информацией в небезопасном глобальном Интернете. Здесь мы рассмотрим очень простой, чисто иллюстративный пример. Предположим, есть компания, в которой работает большой штат ком­мивояжеров. У каждого из них есть корпоративный ноутбук. Далее предположим, что эти коммивояжеры должны регулярно обсуждать конфиденциальную корпоративную информацию (например, о це­нообразовании и о товарах). Эта информация хранится на сервере в штаб-квартире компании. Кроме того, допустим, что коммивояжеры также должны пересылать друг другу конфиденциальные документы. Как решить все эти задачи при помощи IPsec? Вы уже догадались, что нужно установить IPsec и на сервере компании, и на ноутбуках у всех коммивояжеров. Тогда всякий раз, когда коммивояжеру потребуется связаться с сервером или с другим коллегой, такой сеанс будет безо­пасным.