Введение

Цель настоящего пособия — осветить процесс информационного обмена по современным протоколам с самого нижнего уровня.

Основное внимание уделено протоколам семиуровневой модели OSI. Описание всех уровней построено по принципу решения инженерной задачи — организации сетевого обмена. Сначала описывается решение задачи «в лоб», описываются его недостатки, предлагается новый уровень, решающий их, аналогично рассматриваются его недостатки и т. д.

Отдельно описаны ключевые протоколы прикладного уровня, используемые сегодня в Интернете.

Рассмотрены некоторые вопросы безопасности информационного обмена, описаны способы его обеспечения.

1 Сетевое взаимодействие по 7-уровневой модели OSI

1.1. 1-й уровень — физический

Представим, что два компьютера хотят осуществить обмен данными. Первое, что для этого необходимо сделать, — соединить их физически, например, с помощью кабеля (рис. 1).

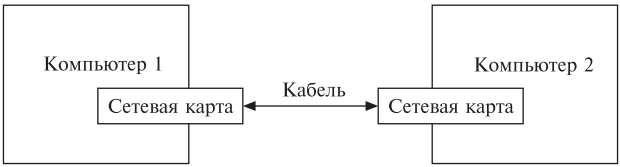

Рис. 1. Физическое соединение

Кроме этого, необходимо договориться о структуре сигнала: несущей частоте, виде модуляции и др. Другими словами, стороны должны одинаково представлять 1 и 0 в виде электрического сигнала.

На этом мы завершили реализацию 1-го уровня модели OSI, который называется *физическим*, поскольку именно он отвечает за задачу физической передачи сигнала.

Если речь идет о беспроводных сетях, то физический уровень отвечает за те же самые вопросы: вид радиосигнала, его модуляция и т. п.

На самом деле этого уже достаточно для того, чтобы стороны могли вести информационный обмен. Теоретически на этом можно было бы остановиться — с трудностями, но обмен данными уже можно вести.

Однако такая простая реализация несет в себе много проблем. Для их решения и созданы следующие уровни модели OSI.

За физический уровень в компьютере отвечает сетевая карта (для проводных соединений) или беспроводной адаптер (для беспроводных). Именно в этих устройствах содержится модулятор и демодулятор сигналов.

1.2. 2-й уровень — канальный

Представим, что теперь у нас не два, а три участника обмена (рис. 2).

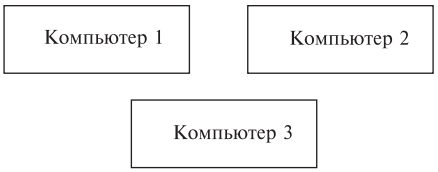

Рис. 2. Три участника обмена

Нам необходимо обеспечить связь таким образом, чтобы каждый мог связаться с каждым. Что для этого нужно? Нужно каждого соединить с каждым (рис. 3).

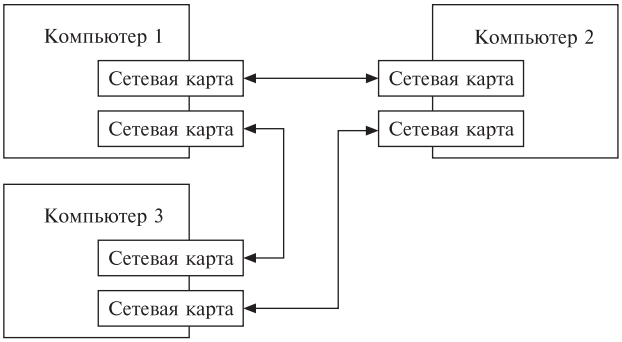

Рис. 3. Соединение трех участников

Когда участников обмена более двух, появляется задача выбора адресата. Допустим, компьютер 1 хочет отправить данные компьютеру 3. Как это обеспечить? В данном случае необходимо передать информацию с помощью именно той сетевой карты, которая ведет к сетевой карте компьютера 3 (рис. 4).

Опять же такой простой способ решения задачи адресации работает, но он сопряжен с рядом проблем.

Во-первых, если всего участников обмена N, то каждому участнику обмена необходимо иметь $N-1$ сетевую карту. То есть, допустим, если участников — 20, то у каждого должно быть установлено 19 сетевых карт.

Во-вторых, число кабелей тоже будет большим: $N(N-1)/2$. Например, для 100 компьютеров необходима прокладка 4950 кабелей.

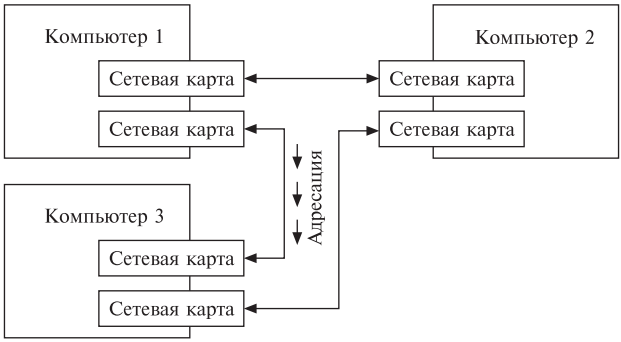

Рис. 4. Адресация

Разумеется, в реальной жизни это невозможно, поэтому было найдено другое решение проблемы. Им стало подключение компьютеров по определенной топологии. Существуют разные виды: кольцо, общая шина и другие. Однако наибольшее распространение получила схема «звезда» (рис. 5).

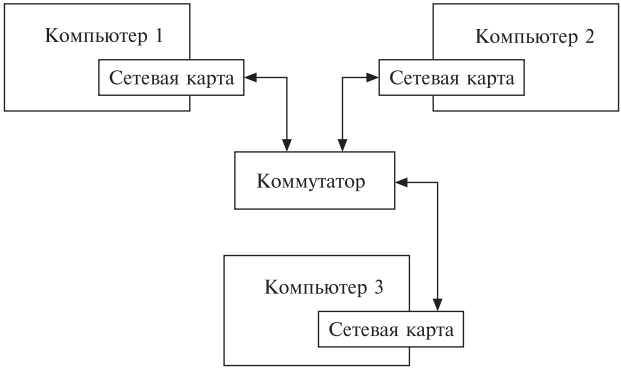

Рис. 5. Соединение через коммутатор

В центре рис. 5 изображено специальное устройство, называемое коммутатором. Другие используемые названия: хаб, свитч, концентратор. По сути он представляет из себя небольшой компьютер со множеством сетевых разъемов (портов). Его задача — перенаправлять пакеты между портами. Таким образом, от каждого участника обмена до коммутатора необходимо проложить всего один провод.

Кроме того, при такой топологии могут образовываться иерархичные структуры, когда один коммутатор является одним из узлов другой сети и так далее. Об этом будет рассказано ниже.

Однако в такой ситуации неизбежно встает вопрос: как теперь адресовать сетевые пакеты? В ситуации, когда у каждого узла сети был индивидуальный провод ко всем остальным узлам, адресация могла быть выполнена по принципу «передаю пакет по тому проводу, к которому подключен адресат». Теперь такой вариант невозможен.

В связи с этим было решено каждому из участников обмена присвоить некий адрес. По сути это просто число, уникальное в пределах одной сети.

Теперь, когда необходимо отправить пакет, в него необходимо добавить адрес узла, которому он адресуется.

Так у нас появился второй уровень информационного обмена — в терминах модели OSI его называют канальным.

Теперь структура движения пакета с данными выглядит так, как на рис. 6.

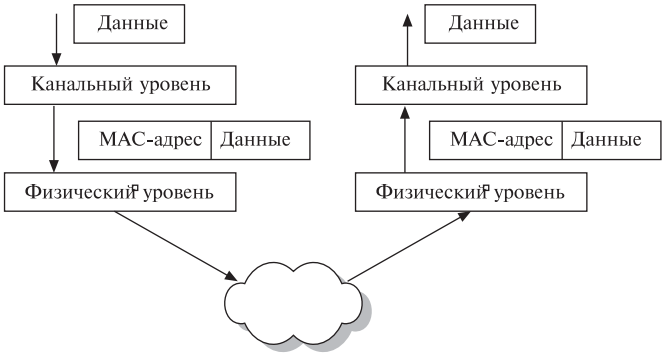

Рис. 6. Появление канального уровня

Как видно, при желании отправить пакет определенному участнику мы передаем его драйверу сетевой карты, попутно сообщая его адрес. Сетевая карта самостоятельно добавляет адрес и передает пакет на физический уровень — для физической передачи по кабелю (об этом было рассказано выше).

Что происходит на получающей стороне? Сетевая карта анализирует каждый полученный пакет. Если в заголовке пакета указан ее адрес, то она извлекает его и передает на уровень выше — в данном случае непосредственно тому, кому предназначается информация.

Если же адрес в заголовке не соответствует адресу сетевой карты, то она просто игнорирует его и не передает дальше на обработку.

Адрес представляет из себя 6-байтовое число и называется MAC-адресом. Аббревиатура расшифровывается как Media Access Control — управление доступом к среде. Обычно его записывают в шестнадцатеричной форме:

00-50-56-C0-00-08

MAC-адрес также часто называют физическим адресом.

Изначально предполагалось, что MAC-адрес будет жестко запрограммирован в сетевой карте и не сможет быть изменен. Специальная схема выдачи MAC-адресов предполагала, что в мире не будет двух любых сетевых карт с совпадающим адресом. К примеру, часть адреса являлась фиксированной для одного производителя, а он уже сам распределял выделенный ему диапазон адресов. За счет того, что часть адреса, присвоенная производителю, у всех производителей тоже была уникальна, обеспечивалась независимость алгоритмов присвоения адресов внутри завода.

Первоначально действительно MAC-адрес был запрограммирован жестко и не подлежал изменению. Однако позже появилась возможность смены этого адреса. Например, для встроенных в материнскую плату сетевых карт было позволено менять адрес через BIOS. Позже такая возможность была добавлена непосредственно в конфигурацию драйвера, таким образом, адрес можно было сменить прямо из операционной системы. Аналогичный принцип был использован и во внешних сетевых картах.

Такая трансформация потребовала изменений и в некоторых информационных системах. Так, например, когда MAC-адреса нельзя было менять, на них часто была основана идентификация компьютеров в сети при раздаче Интернет-трафика (который в ту пору был платный и тарифицировался помегабайтно). Почему использовались именно физические адреса, а не IP-адреса (о них будет сказано ниже)? Дело в том, что IP-адрес можно было легко поменять и «представиться» другим компьютером, а MAC подделать тогда было невозможно.

С появлением перепрограммируемых MAC-адресов стали возникать и случаи мошенничества (воровства чужого предоплаченного трафика). Это потребовало изменения подхода к аутентификации пользователей — например, стали активно применять VPN-подключение.

Посмотреть физический адрес сетевых карт своего компьютера можно с помощью командной строки, набрав команду

ipconfig /all

1.3. 3-й уровень — сетевой

Описанная выше адресация значительно облегчила сетевое взаимодействие. Однако часть проблем по-прежнему оставались нерешенными.

Допустим, Вася хочет отправить пакет с информацией Пете. Однако при передаче пакета драйверу сетевой карты не получится указать, что он для Пети, — сетевая карта попросту не оперирует такими понятиями. Необходимо указать MAC-адрес Пети.

Для этого необходимо иметь справочник соответствий: у Пети — адрес такой-то, у Вани — такой-то и так далее. В некоторой степени такой справочник очень похож на телефонную книгу.

При отправке пакета необходимо обратиться к справочнику, посмотреть, какой адрес у получателя, и сообщить его сетевой карте вместе с полезной информацией.

Однако при таком подходе возможны трудности. Например, участник по каким-то причинам сменил свой физический адрес (сгорел сетевой адаптер, купил новый компьютер и т. п.). Для того чтобы данные доходили до него, ему необходимо уведомить всех участников информационного обмена о новом адресе. Высока вероятность, что во время рассылки уведомления часть узлов будет недоступна и не получит обновленную информацию. Такие узлы будут по-прежнему пытаться отправлять данные по старому адресу.

Для решения этой проблемы было решено ввести еще один вид адреса — IP-адрес. IP расшифровывается как Internet Protocol.

Если MAC-адрес называют физическим, то IP-адрес можно назвать логическим, поскольку он изначально был создан таким образом, чтобы конфигурироваться на уровне операционной системы.

Теперь каждый участник может записывать в своей «адресной книге» не MAC-адреса, а IP-адреса. Отличие заключается в том, что при смене MAC-адреса можно оставить прежним IP-адрес, поскольку он конфигурируется в операционной системе и не зависит от сетевой карты. Другими словами, сетевая карта вообще не знает о том, что есть IP-адреса, — это уже уровень операционной системы.

Таким образом, теперь перед отправкой пакета операционная система добавляет к нему IP-адрес, драйвер сетевой карты — MAC-адрес и т. д.

Схема взаимодействия дополнилась новым, 3-м уровнем — *сетевым*. Теперь ее можно изобразить так, как на рис. 7.

Получатель пакета «раздевает» его в обратном порядке: драйвер сетевой карты интерпретирует и отбрасывает физический адрес,

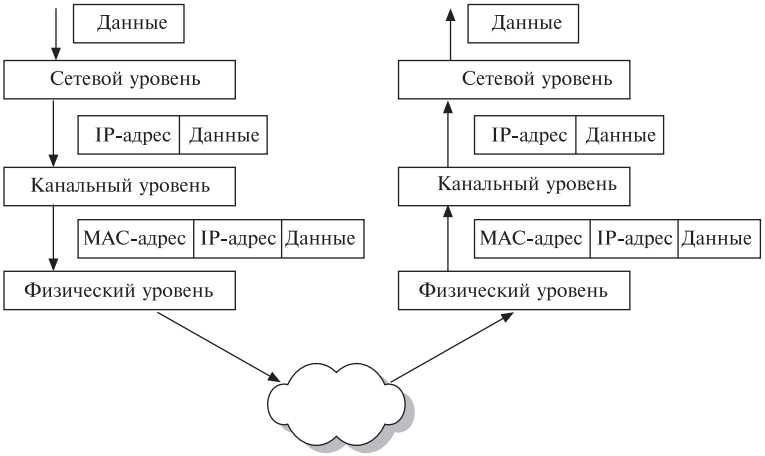

Рис. 7. Появление сетевого уровня

операционная система интерпретирует и отбрасывает IP-адрес, возвращая пользователю только полезную нагрузку.

IP-адрес записывается в виде 4-байтового числа в десятичной форме, разделенного точками:

195.67.38.81

Однако возникает вопрос: мы знаем IP-адрес получателя, но не знаем его MAC-адреса. А для реальной передачи данных физический адрес тоже необходимо знать — ведь на канальном уровне все осталось по-прежнему.

1.3.1. ARP-запросы

Для решения этой задачи существует специальная таблица, в которой указано соответствие между IP-адресами и MAC-адресами. Такая таблица называется ARP-таблицей (Address Resolution Protocol — протокол определения адреса) и выглядит примерно так, как показано в табл. 1.

Таблица 1

ARP-таблица

IP-адрес	MAC-адрес
192.168.127.254	00-50-56-fa-e9-3e
224.0.0.2	01-00-5e-00-00-02

Однако как узнать данные, чтобы заполнить такую таблицу? Для этого используются ARP-запросы. Это специальные пакеты,