

Глава 1

Числа и Сеть сетей

Интернет создали в 1970-х годах в США на случай глобальной ядерной войны. «Сценаристы» Пентагона предсказывали очень неприятный расклад: после массированного ядерного удара по США инфраструктура систем связи будет разрушена и уцелеет лишь несколько командных центров-бункеров, разбросанных по огромной территории. Этим центрам нужно будет установить связь между своими компьютерными сетями, используя остатки инфраструктуры.

Невозможно заранее предсказать, какие кабельные и радиорелейные линии связи сохранят работоспособность и какие пути окажутся доступными для доставки данных из одного командного пункта в другой. Более того, нельзя предвидеть, какие командные центры уцелеют после ядерного удара. Все это усложняло задачу, решение которой в итоге дало миру Интернет.

Другими словами, Интернет придумали как саморегулирующуюся сеть компьютерных сетей — сумму телекоммуникационных технологий, призванных обеспечивать надежность межсетевого взаимодействия в масштабе стран и огромных территорий.

Древний Интернет... Да, именно древний. Это вполне допустимый термин: по меркам суперскоростного прогресса в сфере информационных технологий Интернет действительно древнее явление. Итак, древний Интернет в плане адресации был числовым, потому что его придумали специалисты в области компьютерных технологий, а, как известно, компьютеры очень любят разнообразные числа и не любят слова и естественные языки. Более того, именно использование правильного числового представления позволило создать саморегулирующуюся сеть передачи данных. Числами обозначались адреса подключенных к Интернету компьютеров. С помощью преобразования чисел компьютеры находили пути доставки данных друг другу внутри Интернета.



В основе функционирования современного Интернета, конечно, также лежат числа. Однако современному массовому пользователю они не видны и скорее напоминают некий реликт, тайный артефакт, направляющий глубинные процессы внутри Глобальной сети.

КСТАТИ



Важно понимать, что все межкомпьютерные процедуры по обмену данными реализуются исключительно в числовом виде и могут быть сведены к математическим операциям по «превращению» одних чисел в другие и по установлению сравнительных отношений между числами (больше, меньше, равно). Когда речь идет о компьютерной технике, то буквенные обозначения всегда появляются лишь для удобства работающих с компьютерами людей. Но буквенные обозначения **рано или поздно появляются обязательно**.

Каждый компьютер, подключенный к Интернету, идентифицируется специальным адресом — так называемым IP-адресом. Проще говоря, IP-адрес позволяет отличить один узел от другого.

IP-адреса, конечно, задаются в цифровой форме — в современной версии они состоят из 32 бит. IP-адрес можно записать с помощью нескольких чисел в десятичной системе счисления. Например, 192.168.35.101 или 10.10.101.123. IP-адреса компьютеров соответствуют протоколу IP, являющемуся неотъемлемой частью группы протоколов TCP/IP. В свою очередь, TCP/IP — один из ключевых элементов, обеспечивающих передачу данных между сетевыми узлами Интернета.

Протоколы обмена данными — это некоторые стандарты, определяющие, каким образом компьютеры должны воспринимать и преобразовывать числа, представляющие собой передаваемые данные. Например, в определении протокола описано, какие части принятого (или переданного) пакета данных представляют собой служебную информацию, а какие — собственно полезные данные. Для успешного обмена данными компьютеры должны использовать совместимые протоколы, а если упростить ситуацию, то можно сказать, что компьютеры должны использовать один и тот же протокол.

Протокол IP, входящий в состав группы TCP/IP, определяет адресацию сетевых узлов в Интернете и задает правила доставки пакетов данных от узла к узлу. При этом на своем пути пакеты данных могут фрагментироваться (то есть разбиваться на части) и собираться вновь в единое целое.

Общие принципы, на которых строится процесс доставки данных в Интернете, можно представить с помощью такого примера. Предположим, что из одного города в другой перемещают крупный машиностроительный завод. Перевезти завод целиком невозможно: нет такого вида транспорта. Поэтому завод сперва «размонтируют», разбирают на составные элементы. Элементы перевозят к новому месту, где из них собирают завод.

При этом элементы завода можно перевозить самыми разными видами транспорта. Например, мебель из столовой отправляется на грузовике. Небольшие металлообрабатывающие станки — железнодорожным транспортом, потому что в грузовики они не

влезают. А для перевозки огромного парового пресса требуется грузовое судно речного флота, так как для железной дороги этот пресс — негабаритный груз. Впрочем, если к месту нового расположения завода грузовое судно не может добраться, то для доставки пресса придется использовать другой вид транспорта.

Элементы завода прибывают к месту сборки в разном порядке, так как у различных видов транспорта разная скорость. При этом завод нужно собрать правильно.

Обмен данными в Интернете по протоколам TCP/IP происходит похожим образом. Только вместо различных видов транспорта здесь используются разные каналы связи (доступные в данный момент времени), и сборку-разборку пакетов данных осуществляет не бригада монтажников, а компьютерная программа, реализующая протокол обмена данными. Выбор путей доставки данных между двумя узлами происходит по весьма сложным алгоритмам, учитывающим множество факторов, среди которых, например, загруженность каналов связи на заданном направлении, стоимость доставки пакета данных.

Числа, составляющие IP-адрес, определяют не только узел Интернета, но и сеть, к которой принадлежит этот узел, ведь Интернет — это сеть сетей.

Впрочем, с увеличением числа пользователей компьютерных сетей выяснилось, что числа привычны лишь небольшой части пользователей. Поэтому неудивительно, что еще в начале 80-х годов XX века возникли трудности с практическим использованием чисел, определяющих адреса в Интернете.

Первопричиной прихода буквенных, точнее, алфавитно-цифровых обозначений в систему адресации Интернета стала электронная почта. Оказалось, что людям гораздо проще было бы представлять адреса электронной почты в виде, сходном с адресами обычной почты. Понятно, что удобство записи и запоминания адресов способствует росту эффективности использования

электронной почты. Поэтому на смену сложным комбинациям чисел пришли адреса вида `alex.ivanov@test.ru`.

Конечно, системы, преобразовывающие числовые адреса в символьные строки, в компьютерных сетях были известны и ранее, до возникновения электронной почты. Более того, некоторые из этих систем использовались даже до появления TCP/IP. Тем не менее именно межсетевое распространение электронной почты подтолкнуло инженеров к идее введения общей системы символьной адресации в Интернете. Так в 1983 году появилась система доменных имен Интернета — **DNS (Domain Name System)**.

DNS представляет собой сложный распределенный технологический механизм, позволяющий сопоставить символьному имени домена один или несколько числовых IP-адресов, определяющих соответствующий узел Интернета. Например, `test.ru = 192.168.17.101`, то есть доменному имени `test.ru` соответствует адрес `192.168.17.101`.

Домены для Интернета придумал Пол Мокапетрис (Paul Mockapetris), ученый из США. Именно он разработал основополагающие для DNS документы — RFC 882 и RFC 883.

КСТАТИ



RFC (Request for Comments) — достаточно свободная форма определения тех или иных стандартов и протоколов работы Интернета, сложившаяся в результате исторического развития интернет-сообщества. Большая часть документов RFC, касающихся Интернета, — это описания новых интернет-технологий, добровольно принимаемые ко вниманию и исполнению всеми заинтересованными разработчиками.

В современном Интернете документы RFC 882 и RFC 883 (их тексты опубликованы на специальном сайте: <http://tools.ietf.org/html/rfc882> и <http://tools.ietf.org/html/rfc883>) не действуют — их заменили более новые версии RFC. Однако по фундаментальным принципам работы современная DNS Глобальной сети не отличается от системы, предложенной четверть века назад.

В наше время Интернет обычно ассоциируется с веб-сайтами. Большинство новых пользователей вообще не слышали о других технологиях Интернета, для них понятия веб и Интернет эквивалентны. Но если старые технологии типа Gopher давно умерщвлены всемогущим вебом, то DNS только окрепла, ведь именно символьные имена позволяют вебу виртуализировать понятия реального мира, отражая их в именах доменов.

Современные пользователи Интернета давно привыкли к символьным именам. Подавляющему большинству даже в голову не придет набирать в адресной строке браузера загадочную цепочку чисел вместо понятного <http://nic.ru/>. Текстовые имена проще воспринимаются в рекламе. Адреса сайтов, заданные в виде доменных имен, могут привязываться не только к названию бренда (что необходимо для корпоративных сайтов), но и к той отрасли, к тому сектору рынка, с которым связан сайт. Примерами подобных говорящих имен могут быть и auto.ru, и gramota.ru.

То есть без символьного именования сайтов Интернета никакого интернет-бума быть не могло: ни первого, ни второго. Скорее всего, после очередного «схлопывания инвестиционного пузыря» (а оно неминуемо наступит) в выигрыше останутся держатели доменного пространства как единственной технологии, позволяющей через языковые конструкции мертвым узлом привязать виртуальный мир к реальному.

Глава 2

Обнаружение адреса

DNS преобразует строки символов в IP-адреса. Неспециалистам, оперирующим «банальной эрудицией», этот процесс часто кажется простым. Действительно, возьмите таблицу соответствий «домен — адрес» и работайте по ней — предлагают они. Первые системы прото-DNS так и были устроены. Но в масштабах Глобальной сети это простое решение вполне предсказуемо оказывается неверным.

Например, изменяется соответствие IP-адресов и имен доменов. Для этого есть целый ряд причин. Скажем, домен может сменить владельца, и новый администратор захочет настроить соответствие имен и адресов таким образом, чтобы домен указывал на его сетевой узел, а не на узел старого владельца домена. В маленькой локальной сети из десяти компьютеров, содержащей два собственных домена, наверное, нет проблем с тем, чтобы разослать измененную таблицу соответствия всем десяти компьютерам. Но когда речь идет о сотнях миллионов доменов, помноженных на сотни миллионов компьютеров, разбросанных по всему земному шару, идея с рассылкой общей таблицы имен доменов оказывается, мягко говоря, абсурдной. А ведь нужно учитывать постоянный бурный рост Интернета. Так что реально работающая DNS устроена непросто.

Можно сказать, что IP-адресация формирует из множества узлов Интернета одноуровневую структуру. Узлы в ней соединяют различным образом проложенные линии связи.

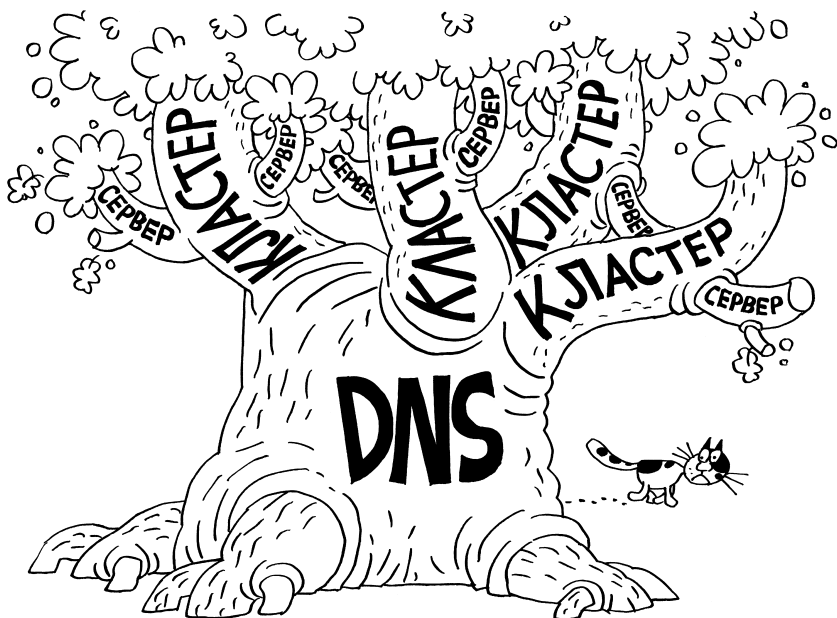
КСТАТИ



По-научному упомянутая плоская структура Интернета со связями между узлами называется графом. А методы успешной и эффективной передачи данных между узлами глобальной Сети помогает разработать в том числе и такая математическая дисциплина, как теория графов. Графы в качестве математического понятия появились задолго до возникновения Интернета — они служили удобным инструментом для исследования сетей электроснабжения.

DNS представляет собой иерархическую древовидную структуру, разбивающую одноуровневое множество узлов (или серверов) Интернета на «отдельные районы» — кластеры. Каждый такой кластер может состоять из многих тысяч серверов или включать в себя только один сервер. Кластеры могут пересекаться, то есть один и тот же узел-сервер может входить в несколько кластеров.

Несложно догадаться, что доменом является узел древовидной структуры DNS. В свою очередь, те серверы Интернета, которые попали в соответствующий узлу кластер, оказываются внутри данного домена. В древовидной структуре DNS каждому узлу дерева соответствует один кластер узлов Интернета. Можно сказать, что дерево DNS как бы добавляет адресной системе Интернета третье измерение, ведь в иерархии доменных имен кластеры вкладываются друг в друга, образуя несколько уровней.



Деление дерева DNS по уровням (первый, второй, третий и т. д.) — важнейшая особенность отношений, возникающих вокруг доме-

нов. DNS, как и всякое дерево, начинается с единственного корневого домена (нулевой уровень). Правда, современная реализация DNS позволяет не указывать корневой домен в адресной строке. Благодаря этому о существовании корневого домена сейчас помнят только специалисты.



КСТАТИ

Адресная строка с указанием корневого домена выглядит, например, так: `site.test.ru.` — здесь корневой домен отделен последней, крайней справа, точкой.

Адреса сайтов с использованием DNS записываются в виде последовательности, отражающей только что рассмотренную иерархию имен. Чем выше уровень домена, тем правее он записывается в строке адреса. Разделяются домены точками. Разберем, например, строку `www.site.nic.ru.` Здесь домен `www` — это домен четвертого уровня, а другие упомянутые в адресной строке домены расположены в домене первого уровня `RU`. Так, `site.nic.ru` — домен третьего уровня. Очень важно понимать, что привычный адрес веб-сайта, скажем, `www.test.ru`, обозначает домен третьего уровня (`www`), расположенный внутри домена второго уровня `test.ru`.

Работу DNS в масштабах всего Интернета обеспечивает распределенная система из многих серверов, которые образуют собственную иерархию. Каждый сервер DNS имеет свою зону ответственности, то есть за ним закреплен участок адресного пространства DNS, в котором этот сервер определяет соответствие IP-адресов и доменных имен. У каждого сервера DNS есть и свой набор клиентов — сервер предназначен для обслуживания именно их.

Основываясь на специальных правилах «доверия» и используя особые протоколы, серверы глобальной DNS обмениваются между собой информацией об изменениях в адресации. При этом изменения не отражаются на всех серверах моментально — напротив, для распространения информации об изменениях в адресации для того или иного домена по всему Интернету может потребоваться несколько суток.

Среди всех серверов DNS есть самые важные — корневые серверы системы, обеспечивающие работу DNS в целом. Таких серверов 13, и они принадлежат техническому центру корпорации ICANN, контролирующей адресное пространство Интернета (подробнее об ICANN и ее регулирующей роли я расскажу ниже).

КСТАТИ



Ни один из 13 корневых серверов DNS не является простым отдельным компьютером, как может показаться. В реальности они представляют собой сложные системы из многих компьютеров, способные одновременно обрабатывать огромное количество запросов. При этом выход из строя даже нескольких составляющих систему компьютеров не приводит к отказу системы в целом.

Ключевую роль играют также корневые серверы доменов первого уровня (например RU), обеспечивающие распространение по всему Интернету DNS-информации о домене, находящемся в их зоне ответственности.

Сложности в построении работающей DNS направлены на то, чтобы каждый из сотен миллионов разбросанных по всему миру компьютеров, подключенных к Интернету, имел возможность корректно преобразовывать адреса.

В упрощенном виде алгоритм работы DNS по поиску адресов веб-сайтов можно описать следующим образом. Когда пользователь вводит в адресной строке браузера адрес веб-сайта, например <http://site.nic.ru/>, компьютер «спрашивает» у того или иного известного этому компьютеру сервера DNS, какой IP-адрес связан с доменным адресом, указанным пользователем. В ответ сервер DNS, проверив соответствие по своим внутренним таблицам или выполнив запрос к другим серверам DNS, присылает искомый IP-адрес. Далее браузер устанавливает соединение с веб-сайтом уже по IP-адресу.

С DNS связано множество проблем безопасности, актуальных как для клиентских компьютеров, так и для Интернета в целом. Например, продвинутые хакеры могут проводить атаки на сервер

DNS, чтобы создать его перегрузку, что вызовет отказы в обслуживании. Подмена адресов в таблицах DNS может приводить к тому, что пользователи, набирающие в адресной строке привычное имя домена, ранее привязанное к одному сайту, будут соединяться с другим сервером, например с сервером злоумышленников, представляющим собой поддельный интернет-магазин, собирающий данные о кредитных картах посетителей.

Проблемы безопасности в DNS в основном связаны с тем, что в восьмидесятых, когда эта система создавалась, Интернет был другим. О многих атаках, ставших возможными теперь, в годы становления Глобальной сети даже не задумывались.

Тем не менее DNS активно развивается и, очевидно, продолжит оставаться ключевым элементом Интернета долгие годы. Несомненно, сохранится и определяющая роль DNS в привычных массовому пользователю механизмах адресации.

В настоящее время к услугам рядового пользователя Глобальной сети — три механизма перехода к тому или иному сетевому ресурсу.

- ❑ Во-первых, пользователь может набрать адрес интересующего сайта в адресной строке браузера.
- ❑ Во-вторых, можно перейти на сайт с помощью поисковой машины, нажав ссылку на странице результатов поиска документов в Интернете.
- ❑ Наконец, третий вариант — переход по ссылке с одного сайта на другой.

На практике в современном Интернете эти три механизма базируются на DNS и доменных именах.

Меняются технологии размещения информации в Интернете, развивается веб, появляются новые средства, позволяющие создавать все более оригинальные веб-сайты. Но пока ни одна из технологий не смогла предложить новых, столь же удобных пользователю механизмов адресации, способных потеснить систему доменных имен.