Модуль 5. Основы разработки серверной части мобильных приложений

Тема 5.1. IP сети

2 часа

Оглавление

5.1. IP сети

Прежде чем перейти к изучению тем по клиент-серверной разработке приложений остановимся кратко на основных понятиях, связанных с Интернет и протоколами, которые обеспечивают его работу.

5.1.1. Об Интернете и протоколах TCP/IP

Американский ученый Л. Клейнрок в июле 1961 г. опубликовал первую статью по теории пакетной коммутации. Проще говоря, он предложил передавать данные через сети, разделив их сначала на небольшие пакеты в несколько десятков байт и потом в адресате из них собирать исходное сообщение. В 1969 году его коллектив в Калифорнийском университете и ученые Стэнфордского исследовательского института впервые продемонстрировали передачу данных с использованием набора сетевых протоколов TCP (Transmission Control Protocol). Пакет данных прошел по маршруту Сан-Франциско – Лондон – Университет Южной Калифорнии и не потерял ни одного бита! Этот день 29 октября 1969 года некоторые историки предлагают считать днем рождения Интернета.

Что же такое Интернет протокол? Протокол – это набор правил, по которым взаимодействуют компьютеры между собой. Без протоколов не было бы Интернета, потому что устройства в сети не понимали бы друг друга.

В 1978 году TCP был разделен на две отдельные группы:

- за разбивку передаваемого сообщения на пакеты данных и их сборку в пункте получения стал отвечать TCP
- за передачу пакетов данных с контролем получения – IP протокол (Internet Protocol).

По отношению к протоколам TCP/IP употребляют термин “стек протоколов”. Почему? Потому что сейчас это уже множество протоколов, которые как бы слоями покрывают друг друга: верхние работают на высоком логическом уровне, не вдаваясь в подробности, которые задают протоколы более низкого уровня. Сейчас в стеке протоколов TCP/IP по одной из классификаций выделяют 4 уровня:

1. **Application layer**. Самый верхний прикладной уровень, где работают протокол HTTP для WWW, FTP (передача файлов), SMTP (электронная почта), DNS (преобразование символьных имён в IP-адреса) и многие другие.
2. **Transport layer**. Протоколы транспортного уровня TCP, UDP решают задачу безошибочной передачи пакетов данных и определяют для какого конкретно приложения они предназначены.
3. **Internet layer**. IP протоколы сетевого уровня занимаются определением, каким кратчайшим путем передавать пакеты, переводит логические адреса и имена в физические и др. На этом уровне работает такое сетевое устройство, как маршрутизатор.
4. **Link layer**. Самый приближенный к физическим устройствам канальный уровень протоколов решает задачу передачи данных узлам, находящимся в том же сегменте локальной сети. Примером протокола этого уровня является Ethernet.

5.1.2. Адресация в IP-сетях

Для функционирования протоколов TCP/IP используются три типа адресов:

- MAC-адрес (физический адрес)
- IP-адрес (сетевой адрес)
- DNS-имя (символьное доменное имя)

MAC-адрес (от Media Access Control) – это уникальный идентификатор, присваиваемый каждой единице активного оборудования, или некоторым их интерфейсам в компьютерных сетях Ethernet[1].

Например, свой MAC-адрес есть как у адаптера беспроводной сети wi-fi, так и у адаптера проводной сети Ethernet. MAC-адрес – это шестибайтный номер, обычно представленный в шестнадцатиричной системе счисления, который выглядит, например, так: EC:89:F5:1A:E6:34 или так: 6C-62-6B-00-FA-D2. Уникальность MAC-адресов достигается тем, что каждый производитель оборудования получает некоторый диапазон из шестнадцати миллионов адресов в координирующем комитете IEEE Registration Authority. По трём старшим байтам MAC-адреса можно определить производителя, младшие же 3 байта назначаются самим производителем. Таким образом, MAC-адреса формируют основу сетей на канальном уровне, которую затем используют протоколы более высокого (сетевого) уровня.

IP-адрес (от Internet Protocol Address) – представляет собой основной тип адресов, с помощью которых происходит обмен пакетами на сетевом уровне. Эти адреса состоят из 4 байт, обычно представленных в десятичной системе счисления, например: 195.208.64.58. IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

DNS-имя (Domain Name System) – символьный идентификатор-имя, такой как, например, myitschool.ru. Доменное имя представляет буквенные адреса, которые гораздо удобнее для восприятия и использования, чем последовательность цифр IP-адреса.

5.1.3. Версия интернет протокола IPv4

В настоящее время IP-адрес может быть задан в двух форматах: IPv4, который имеет длину 4 байта, например: 192.168.0.5, и протокола IPv6, имеющий длину 16 байт, например: 2001:0:5ef5:79fb:208d:201:4db5:a1d4.

Протокол IPv4 появился в 1981 г. и сейчас это самая используемая версия, но в связи с поистине огромным количеством устройств, подключающихся к сети Интернет, количества адресов, которые можно закодировать в 4 байтах, уже не хватает для всех желающих. Поэтому была запущена версия протокола IPv6, способная предложить значительно большее количество уникальных адресов. В настоящее время она только начинает использоваться, на конец 2013 года доля IPv6 в сетевом трафике составляла около 3%, однако этот протокол уже поддерживается всеми современными операционными системами и производителями оборудования. После того, как адресное пространство в IPv4 закончится, два стека протоколов IPv6 и IPv4 будут использоваться параллельно, с постепенным увеличением доли трафика IPv6, по сравнению с IPv4.

Вернёмся к более актуальному на сегодняшний момент протоколу IPv4 и рассмотрим его подробнее. Проанализируем, например, адрес:

192.168.104.115

В этих числах закодированы номер сети и номер узла (компьютера) в сети. Для того чтобы выделить эти две части из IP-адреса, используют маски подсети.

Маска подсети – битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети (при этом, в отличие от IP-адреса, маска подсети не является частью IP-пакета) [2].

Подобно IP-адресу, маска тоже состоит из четырёх чисел в диапазоне от 0 до 255 включительно, но она строится особым образом, по принципу: «n единиц, потом – нули» в двоичном коде. Маску подсети “накладывают” на IP-адрес и получают адрес подсети. Операция наложения маски – это поразрядное логическое И. Поэтому в разрядах, где стоят 1 значение соответствующих разрядов в IP-адресе не изменится, а там, где 0 – обнулится.

Пример 1

Имеем IP-адрес 192.168.104.115 и маску подсети 255.255.255.0, которая в двоичном виде имеет вид:

11111111.11111111.11111111.00000000

Это значит, что первые 24 бита адреса – это адрес сети (192.168.104.0), а оставшиеся 8 битов – номер узла (компьютера) в этой сети (115).

Можно использовать другую запись, которая значит то же самое:

192.168.104.115/24 – «/24» говорит о том, что в маске 24 единицы.

В такой сети может быть 254 узла, а не 256, как можно было бы ожидать. Дело в том, что младший адрес (192.168.104.0) используется для обозначения всей сети, а старший (192.168.104.255) – для так называемой широковещательной рассылки (сообщение отправляется всем компьютерам данной сети). Все узлы с адресами от 192.168.104.1 до 192.168.104.254 находятся в той же сети, что и данный компьютер.

Пример 2

Рассмотрим IP-адрес из Примера 1, но с другой маской 255.255.255.248. В двоичной системе она содержит 29 единиц и 3 нуля.

Адрес	192	.	168	.	104	.	115	
	11000000	.	10101000	.	01101000	.	01110	011
Маска	11111111	.	11111111	.	11111111	.	11111	000
	255	.	255	.	255	.	248	

Узел с адресом 192.168.104.115/29 – это узел номер 3 (011_2) в сети 192.168.104.112 ($11000000.10101000.01101000.01110000_2$)

Поскольку на адрес узла отводится три бита (в маске три нуля), в такой сети доступно только $2^3 = 8$ адресов. Учитывая, что два из них специальные (первый – номер сети, последний – широковещательный адрес), в такую сеть может входить не более 6 узлов.

Нужно помнить, что IP-адрес присваивается не компьютеру, а интерфейсу – каналу передачи данных (проводной сетевой карте, wi-fi адаптеру, модему). Поэтому один компьютер может иметь несколько IP-адресов, (например, если на нём установлены две сетевые карты).

Следующие диапазоны IP-адресов («серые» адреса) не используются в глобальной сети Интернет, а рекомендованы для организации локальных сетей:

- 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)

Особый смысл имеет IP-адрес, начинающийся с 127 – он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы «петля». Данные не передаются по сети, а возвращаются как только что принятые. Этот адрес имеет название loopback. На самом деле для обозначения «самого себя» можно использовать не только 127.0.0.1, но и любой адрес из диапазона от 127.0.0.1 до 127.255.255.254.

Номера сетей назначаются либо централизованно, если сеть является частью Internet, либо произвольно, если сеть работает автономно. Номера узлов и в том и в другом случае администратор волен назначать по своему усмотрению, не выходя, разумеется, из разрешенного для этого класса сети диапазона.
Координирующую роль в централизованном распределении IP-адресов до некоторого времени играла организация InterNIC (Internet Network Information Center), однако с ростом сети задача распределения адресов стала слишком сложной, и InterNIC делегировала часть своих функций другим организациям и крупным поставщикам услуг Internet. Обычно поставщики услуг Internet получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между своими абонентами.

5.1.4. Автоматизация процесса назначения IP-адресов

При создании локальной сети администратору необходимо назначить IP-адреса всем устройствам сети. Эта задача определяется протоколом Dynamic Host Configuration Protocol (DHCP) и может быть решена тремя способами:

1. **Вручную**. Даже при не очень большом размере сети это довольно утомительно.
2. **Автоматически**. Администратор только задает диапазон, из которого должны быть назначены IP-адреса. Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP – сервер откликается и посылает сообщение-ответ, содержащее IP-адрес. Конечно, предполагается, что DHCP-клиент и DHCP-сервер находятся в одной IP-сети. Между идентификатором

клиента и его IP-адресом, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первого назначения DHCP-сервером IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

3. **Динамически**. DHCP-сервер выдает адрес клиенту на ограниченное время, называемое временем аренды (lease duration), что дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру.

Основное преимущество DHCP – автоматизация рутинной работы администратора по конфигурированию стека TCP/IP на каждом компьютере.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся DHCP-клиентом, удаляется из подсети. При этом назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных устройств.

DHCP-сервер может назначить клиенту не только IP-адрес клиента, но и другие параметры стека TCP/IP, необходимые для его эффективной работы, например, маску, IP-адрес маршрутизатора по умолчанию, IP-адрес сервера DNS, доменное имя компьютера и т. п.

5.1.5. Доменные имена (DNS), URL-ссылки

Как нам уже известно, для однозначной идентификации узла в сетях TCP/IP используется IP-адрес. Например, укажем в адресной строке браузера адрес http://195.208.64.58, мы попадём на страницу учебного портала IT-школы SAMSUNG. Однако пользователям не очень удобно работать с числовыми адресами. И что делать, если сайт необходимо перенести на другой сервер? Ведь это значит, что IP-адрес сменится и пользователи не смогут найти нашу страницу.

Для решения этих проблем в 1984 г. была разработана система доменных имён (англ. DNS — Domain Name System), которая позволила установить в соответствие определённым IP-адресам некоторые символьные имена, например, myitschool.ru. Это значит, что мы можем менять IP-адрес и при этом доменное имя останется прежним!

В построении доменных имён используется древовидная иерархия. Совокупность имен, у которых несколько старших составных частей совпадают, образуют домен имён (domain). Например, имена myitschool.ru, yandex.ru и mail.ru входят в домен ru, так как все эти имена имеют одну общую старшую часть – имя ru. А вот сайт www.samsung.com/ru/home/ в домен ru не входит, так как он находится в доменной зоне com.

Термин «домен» очень многозначен, поэтому его нужно трактовать в рамках определенного контекста. Кроме доменов имен стека TCP/IP в компьютерной литературе также часто упоминаются домены Windows NT, домены коллизий н некоторые другие. Общим у всех этих терминов является то, что они описывают некоторое множество компьютеров, обладающее каким-либо определенным свойством.

Если один домен входит в другой домен как его составная часть, то такой домен могут называть поддоменом (subdomain), хотя название домен за ним также остается. Обычно поддомен называют по имени той его старшей составляющей, которая отличает его от других поддоменов.

Необходимо подчеркнуть, что компьютеры входят в домен в соответствии со своими составными именами, при этом они могут иметь совершенно различные IP-адреса, принадлежащие к различным сетям и подсетям.

В Internet корневой домен управляется центром InterNIC. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций – следующие обозначения:

- com – коммерческие организации
- edu – образовательные организации
- org – некоммерческие организации
- net – организации, поддерживающие сети
- biz – организации, связанные с бизнесом

Каждый домен администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Распределением IP-адресов и доменов первого уровня занимается международная организация ICANN (англ. Internet Corporation for Assigned Names and Numbers). Российский домен ru был зарегистрирован в 1994 году.

Свободный домен второго уровня может зарегистрировать любой желающий за сравнительно небольшую плату. Домены регистрируются сроком на один год с правом последующего платного продления. Очевидно, регистрацию или приобретение доменов правильнее называть арендой. Такие услуги оказывают специальные организации – регистраторы доменных имён, например RU-Center (nic.ru). Домены третьего уровня, за некоторыми исключениями, не имеют особой ценности и их часто можно арендовать бесплатно.

Раньше в доменных именах было разрешено использовать только латинские буквы, цифры и дефис. Сейчас можно регистрировать домены, содержащие другие знаки, входящие в кодировку UNICODE, например, буквы русского алфавита. За Россией закреплён домен рф, в котором все желающие могут зарегистрировать домены второго уровня.

Таким образом, в Интернете используются две системы адресов: IP-адреса и доменные имена. Чтобы установить соответствие между ними, на специальных серверах, которые называются DNS-серверами, хранятся таблицы, состоящие из пар «IP-адрес – доменное имя». По запросу компьютера-клиента они возвращают IP-адрес для заданного доменного имени (или наоборот).

Для того, чтобы компьютер смог установить связь с сетью, в настройках сетевой карты (или модема) указывается IP-адрес, маска сети и адрес DNS-сервера. Иногда эти данные определяются автоматически при подключении к сети провайдера.

Когда вы вводите адрес сайта (доменное имя) в адресной строке браузера, сначала отправляется запрос на DNS-сервер, цель которого — определить IP-адрес сервера. Если это удалось, направляется запрос на получение веб-страницы, причем драйвер протокола IP использует полученный IP-адрес, а не доменное имя.

Заметим, что одному доменному имени может соответствовать несколько IP-адресов. Такой приём применяется для распределения нагрузки на сайты с большим количеством посетителей (например, www.yandex.ru, www.google.com). Таким образом, соответствие между доменными именами и IP-адресами можно описать как «многие ко многим»: с одним IP-адресом может быть связано несколько доменных имён и наоборот.

Точный адрес имеет не только каждый компьютер в Интернете, но и каждый документ. Для такого адреса чаще всего используется английское сокращение URL – Uniform Resource Locator – универсальный указатель ресурса. Типичный URL-адрес состоит из четырёх частей: протокола, имени сервера (или его IP-адреса), каталога и имени документа (файла). Например, адрес

http://myitschool.ru/is/Education/Markbook.aspx

включает:

- протокол HTTP – протокол для обмена гипертекстовыми документами (это веб-страница)
- доменное имя сервера myitschool.ru
- каталог на сервере /is/Education/
- имя файла Markbook.aspx

Иногда каталог и имя файла не указывают, например: http://myitschool.ru. Это означает, что мы обращаемся к главной странице сайта. Она может иметь разные имена, в зависимости от настроек сервера (чаще всего – index.htm, index.html, index.php).

5.1.6. Сервисы работы с IP-адресами.

WHOIS – сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем. Протокол осуществляет доступ к публичным серверам баз данных регистраторов IP-адресов и регистраторов доменных имён.

Рассмотрим работу протокола WHOIS на примере сервиса RU-CENTER (АО «Региональный Сетевой Информационный Центр») – первого и крупнейшего в России профессионального регистратора доменов. Для этого нужно зайти на сайт http://www.nic.ru и затем выбрать сервис WHOIS (можно просто сразу перейти по адресу http://www.nic.ru/whois/), затем в окне «Для получения информации введите имя домена или IP-адрес:» следует ввести IP-адрес интересующего нас сайта или его доменное имя, например: myitschool.ru. На экран будет выведена информация по IP-адресу или доменному имени, в том числе:

- имя владельца
- имя регистратора
- контактную информацию владельца
- дату регистрации доменного имени

Не меньший интерес представляет сервис http://2ip.ru/. С его помощью можно узнать собственный IP-адрес, а также множество другой информации – имя провайдера, географию вашего местонахождения, используемую операционную систему, версию браузера и т.д.

Также есть возможность протестировать скорость Интернет соединения, выполнить онлайн-команду ping (которую мы подробнее изучим ниже), определить используемую CMS (систему управления сайтом), узнать физическое расстояние от географического расположения одного сайта или IP-адреса до другого, и многое другое.

Упражнение 5.1.1

Узнать собственный внешний IP-адрес с помощью сервиса: http://2ip.ru/. Пояснить, что внешний IP-адрес у всех в комнате одинаковый, так как это адрес компьютера, подключенного к интернету.

В сервисе http://www.nic.ru/whois/ изучить информацию о собственном внешнем IP-адресе. Можно также посмотреть информацию об IP-адресах: 8.8.8.8, 87.240.131.99, 211.45.27.198 или 173.194.71.113.

5.1.7. Популярные сетевые команды

При работе с сетью часто возникают задачи, связанные с проверкой доступности компьютеров и правильности работы службы DNS. Для этой цели администраторы традиционно используют утилиты, работающие из командной строки. В Linux для работы в командной строке нужно запустить программу Терминал (Console), а в Windows – командный процессор cmd. Сделать это в Windows можно следующими способами:

1. Зайти в меню Пуск и выбрать Программы -> Служебные -> Командная строка
2. Зайти в меню Пуск, выбрать Выполнить, в окне Открыть написать cmd и нажать Ок или Enter на клавиатуре.

Теперь у нас есть возможность пользоваться консольными командами. Рассмотрим возможности, которые нам предоставляет этот метод.

Команда ipconfig (ifconfig)

Это одна из самых полезных служебных команд, которая позволяет просмотреть текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений.

Команду ipconfig (для ОС семейства Linux - ifconfig) следует первой использовать для диагностирования возможных проблем с соединением TCP/IP. Чтобы получить справку по всем возможным ключам запустите команду

- в Windows: Ipconfig /?
- в Linux: Ifconfig -help

Наиболее часто используют параметр /all, который позволяет получить большую часть информации, содержащейся в диалоговом окне свойств.

Команда ping

Для того чтобы протестировать работоспособность сети, следует использовать выполнить команду ping. Эта команда отправляет запросы к удаленному компьютеру с использованием при этом специального протокола ECHO. Получив такой запрос, удаленный компьютер сразу же отправляет его обратно по тому адресу, откуда он пришел. Таким образом можно узнать, есть ли вообще связь. В качестве параметра команды можно указывать как IP-адрес, так и доменное имя интересующего нас узла.

Таким образом, команда ping позволяет протестировать соединение между двумя компьютерами на очень низком (физическом) уровне. При успешном возвращении запросов можно быть уверенным в том, что среда передачи данных, программное обеспечение TCP/IP, а также все устройства (маршрутизаторы, повторители и др.), встретившиеся на пути между двумя компьютерами, работают нормально. Необходимо отметить, что даже при отсутствии каких-либо неисправностей на пути между двумя компьютерами, один или сразу несколько пакетов могут быть утеряны, как правило, это связано с перегруженностью сети, а также с тем, что большинство маршрутизаторов отводит диагностирующим пакетам очень низкий приоритет. Если хотя бы один из посланных пакетов вернется, это уже будет означать исправность работы сети.

Для получения справки по команде используйте

- в Windows: ping /?
- в Linux: ping -help

Одним из распространенных вариантов выполнения команды ping является использование параметра -t. Это повторяет запросы к удаленному компьютеру, пока программа не будет остановлена с помощью комбинации клавиш <Ctrl+C>. Как правило, подобная практика бывает полезна при устранении неисправностей сети. Запущенный “бесконечный” тест команды ping наглядно поможет отслеживать результаты каких-либо внесенных изменений.

Запуск команды ping с ключами -n и -l позволит несколько расширить параметры опроса, а именно: ключ -n - указывает фиксированное количество отправляемых пакетов, -l - размер одного пакета-передачи, ограниченного максимальным значением в 64кБ.

Следует также отметить параметр TTL (time to Live - "время жизни пакета"), который может принимать значения 32, 64, 128. Он предусмотрен для того, чтобы при поиске места назначения пакета маршрутизаторы не зацикливались. Как только значение этого параметра превышает допустимое, пакет считается попавшим в цикл и уничтожается.

Команда tracert (traceroute)

Эта команда подобна команде ping: обе команды посылают в точку назначения эхо-пакеты протокола Internet и затем ожидают их возвращения. Главное отличие пакетов команды tracert от пакетов ping заключается в том, что они имеют различный срок жизни. Первые пакеты помечаются специальной меткой, означающей, что они не могут быть пропущены ни одним маршрутизатором. При достижении первого же маршрутизатора на тестируемом пути такие пакеты отсылаются обратно на тестирующий компьютер как пакеты, которые невозможно доставить по данному адресу. Возвращенные пакеты содержат адрес не пропустившего их маршрутизатора, определяя таким образом первое звено в тестируемом маршруте. Обычно им

является либо сетевой шлюз (при подключении к Internet по локальной сети), либо устройство, принимающее модемные звонки в офисе провайдера услуг Internet (при коммутируемом подключении). Затем tracert пересылает следующие пакеты, уже помечая их как пакеты, которые могут быть пропущены не более чем одним маршрутизатором. Таким образом будет определено второе звено в тестируемом маршруте. Количество маршрутизаторов, через которые может пройти пакет, будет каждый раз увеличиваться на единицу до тех пор, пока пакет не достигнет точки назначения. Таким образом, с помощью команды tracert можно получить подробный маршрут прохождения пакетов данных между компьютером, на котором была запущена tracert, и любым удаленным компьютером сети. Это делает tracert весьма ценным средством обнаружения неисправностей в сетевом соединении: в случае возникновения проблемы с подключением к Web-узлу или к какой-нибудь другой службе Internet можно, по крайней мере, определить участок, на котором она возникла.

Для получения помощи по возможным ключам команды используйте

- в Windows: tracert /?
- в Linux (Ubuntu): traceroute --help

Команда nslookup

С помощью команды nslookup можно опрашивать конкретные DNS-серверы по конкретным типам записей DNS.

Для получения помощи по возможным ключам команды используйте

- в Windows: nslookup /help
- в Linux (Ubuntu): man nslookup

При запуске nslookup без параметров, мы попадаем в интерактивный режим, где можно вводить различные команды, доменные имена и IP-адреса. Выход – команда exit или сочетание Ctrl+C.

Можно запускать nslookup с параметрами. Следующая команда должна показать IP-адрес сайта.:

nslookup myitschool.ru

Сообщение "Не заслуживающий доверия ответ:" (Non-authoritative answer:) говорит о том, что выполняющий запрос DNS-сервер, не является владельцем зоны myitschool.ru, т.е. записи для узла myitschool.ru в его базе отсутствуют, и для разрешения имени использовался рекурсивный запрос к другому DNS-серверу.

Команда:

nslookup 195.208.64.58
должна отобразить имя узла, соответствующее введенному IP-адресу.

Упражнение 5.1.2

Опробовать все изученные команды. В процессе выполнения записать IP-адреса популярных сервисов и время ответа на команду ping.

Источники

[1] Википедия. URL: http://ru.wikipedia.org/

[2] Информатика. 10 класс. Углубленный уровень. Часть 2. Поляков К.Ю., Еремин Е.А. М.: 2013, 304с.

[3] Информационные сети. Учебное электронное издание. Т.Т. Газизов. URL: http://koi.tspu.ru/koi_books/gazizov2/

[4] Умные железки. Маслёнков А. URL: http://andreyex.narod.ru/netcom.htm

Благодарности

Компания Samsung Electronics выражает благодарность за участие в подготовке данного материала преподавателю IT ШКОЛЫ SAMSUNG Шелихову Олегу Юрьевичу.